Testing quantum expanders is co-QMA-complete

Adam D. Bookatz[*] Stephen P. Jordan[†] Yi-Kai Liu[‡] Pawel Wocjan[§]

October 2, 2012

Abstract

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 this problem is co-QMA-complete. This has applications to testing randomized constructions of quantum expanders, and studying thermalization of open quantum systems.

1 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 analogues of expander graphs, which play a prominent role in computer science and discrete mathematics [16]. The idea of quantum expanders was introduced in [13, 4]. 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 [5, 14, 11, 12, 15, 8].

Here we study the problem of estimating the mixing rate of a quantum expander. Given a quantum channel Φ of the above form (a small number of Kraus operators, specified by quantum circuits), this problem is to estimate the spectral gap of Φ. This problem arises in connection with randomized constructions of quantum expanders [8],

[*] Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, USA; bookatz@mit.edu

[†] National Institute of Standards and Technology, Gaitherburg, MD, USA; stephen.jordan@nist.gov

[‡] National Institute of Standards and Technology, Gaithersburg, MD, USA; yi-kai.liu@nist.gov

[§] Mathematics Department & Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, USA; on sabbatical leave from Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL, USA; wocjan@eecs.ucf.edu

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 non-expander 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 analogue of NP (Nondeterministic Polynomial Time) [20, 24, 27]. Proving that a problem is QMA-complete implies that it is equivalent (up to polynomial-time reductions) to all other QMA-complete problems [24, 17, 21, 22, 3, 19, 1, 18], a survey of which can be found in [7]. 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," cannot be in QMA (unless QMA = coQMA). In other words, when a channel Φ is *not* a quantum expander, there is an efficiently-verifiable quantum proof of that fact; but when Φ *is* a quantum expander, there is no way of giving an efficiently-verifiable quantum proof.

2 Preliminaries

2.1 The quantum non-expander problem

We use the definition of explicit quantum expanders due to Ben-Aroya, Schwartz, and Ta-Shma [5]. 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 unital if $\Phi(\tilde{I}) = \tilde{I}$, where $\tilde{I} = \frac{I}{N}$ is the maximally mixed state on $\mathcal{H}$ (where I is the identity operator on $\mathcal{H}$). A unital superoperator is D-regular if $\Phi = \frac{1}{D}\sum_d \Phi_d$, 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 Φ, and D is called the degree of Φ. A D-regular superoperator is explicit if each of its operation elements can be implemented by a quantum circuit of size polylog(N), where N is the dimension of $\mathcal{H}$.

Definition 2.1 (Quantum expander). *A D-regular superoperator $\Phi : L(\mathcal{H}) \to L(\mathcal{H})$ is a κ-contractive expander if for all $A \in L(\mathcal{H})$ that are orthogonal to $\tilde{I}$ with respect to the Hilbert-Schmidt inner product, that is,* $\mathrm{Tr}(A\tilde{I}) = 0$*, 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 Φ.

Remark 2.2. The motivation for this definition can easily be seen from the following argument. A good quantum expander Φ rapidly sends any density matrix ρ to the maximally mixed state $\tilde{I}$. Because $\mathrm{Tr}[\rho] = \mathrm{Tr}\left[\tilde{I}\right] = 1$ we can always write $\rho = \tilde{I} + A$ where $\mathrm{Tr}[A] = 0$. The requirement of Eq. (1) therefore formalizes the idea of Φ bringing ρ towards $\tilde{I}$ by rapidly killing off the A term. In this context Eq. (1) is equivalent to demanding that $\left\|\Phi(\rho) - \tilde{I}\right\|_F \leqslant \kappa \left\|\rho - \tilde{I}\right\|_F$, which clearly encapsulates the idea of Φ rapidly sending density matrices towards the maximally mixed state. Note that in this argument $A = \rho - \tilde{I}$ 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 2.1.

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

Definition 2.3 (Quantum non-expander problem)**.** *Fix some encoding such that each string $x \in \{0,1\}^*$ specifies the following: an explicit D-regular superoperator $\Phi : (\mathbb{C}^2)^{\otimes m} \to (\mathbb{C}^2)^{\otimes m}$, with operation elements $U_1, \ldots, U_D$, and two parameters $\alpha > \beta$.*

We will consider instances which satisfy the following promises[1]: m and D are upper-bounded by (fixed) polynomials in $|x|$; the parameters α and β are polynomially separated, i.e., they satisfy $\alpha - \beta \geq \frac{1}{q(|x|)}$ 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 non-expander" problem is the task of deciding which of the following is correct, given the promise that exactly one of them is correct:

- *Φ is not an α-contractive expander (YES case)*
- *Φ is a β-contractive expander (NO case)*

2.2 Thermalization of open quantum systems

To motivate the "quantum non-expander" 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_α (for $\alpha = 1, \ldots, D$) which act on $(\mathbb{C}^2)^{\otimes m}$. Let the bath consist of a large number of harmonic oscillators, with annihilation operators $b_{\alpha k}$ (for $\alpha = 1, \ldots, D$ and $k \in \Omega$, where Ω is some large set). Let the total Hamiltonian be

$$H = H_S + \varepsilon H_I + H_B, \tag{2}$$

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

$$H_B = \sum_\alpha \sum_k \omega_k b_{\alpha k}^\dagger b_{\alpha k}, \tag{3}$$

[1] Here $|x|$ denotes the length of the string x.

and the interaction Hamiltonian is

$$H_I = \sum_\alpha (U_\alpha \otimes f_\alpha) + (U_\alpha^\dagger \otimes f_\alpha^\dagger), \tag{4}$$

where the operators f_α are defined by $f_\alpha = \frac{1}{\sqrt{|\Omega|}} \sum_k b_{\alpha k}$.

In the weak-coupling limit ($\varepsilon \to 0$), the time evolution of the system is described by a master equation [9]. 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:

$$\frac{d}{dt}\rho_S(t) = R_0 \sum_\alpha \Big(U_\alpha \rho_S(t) U_\alpha^\dagger - \rho_S(t) \Big) + R_1 \sum_\alpha \Big(U_\alpha^\dagger \rho_S(t) U_\alpha - \rho_S(t) \Big), \tag{5}$$

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 A.1 for the derivation of this equation.)

Now define the quantum channel

$$\Phi(\rho) = \frac{R_0}{(R_0+R_1)D} \sum_\alpha U_\alpha \rho U_\alpha^\dagger + \frac{R_1}{(R_0+R_1)D} \sum_\alpha U_\alpha^\dagger \rho U_\alpha.$$

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

$$\Phi(\rho) = \frac{1}{D} \sum_\alpha U_\alpha^\dagger \rho U_\alpha,$$

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

The master equation can now be rewritten in terms of Φ:

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

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

$$\rho_S(t) = \exp\Big(t \cdot (R_0+R_1)D \cdot \big(\Phi - \mathcal{I}\big)\Big)(\rho_S(0)).$$

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

$$\|A(t)\|_F \leq \exp\big(-t \cdot (R_0+R_1)D(1-\kappa)\big)\|A(0)\|_F.$$

2.3 Quantum Merlin-Arthur

We will show that the quantum non-expander problem is QMA-complete, i.e., it is contained in QMA, and every problem in QMA can be reduced to it in polynomial time.

The complexity class QMA consists of decision problems such that YES instances have concise quantum proofs. The name QMA stands for Quantum Merlin-Arthur, which is motivated by the following protocol. Given a problem instance x (*i.e.* a string of $|x|$ bits), and a language $L \in QMA$, a computationally unbounded but untrustworthy prover, Merlin, submits a quantum state of poly($|x|$) qubits as a purported proof that $x \in L$. A verifier, Arthur, who can perform polynomial size quantum computations, then processes this proof and either accepts or rejects it. If $x \in L$ then there exists some polynomial size quantum state causing Arthur to accept with high probability, but if $x \notin L$ then Arthur will reject all states with high probability. QMA is a quantum analogue of MA, which is the probabilistic analogue of NP.

Definition 2.4 (QMA(a, b))**.** *A language L is in QMA(a, b) if for each $x \in \{0, 1\}^*$ one can efficiently generate a quantum circuit V with the following properties:*

- *V acts on the Hilbert space $\mathcal{W} \otimes \mathcal{A}$ where*

  $$\mathcal{W} = (\mathbb{C}^2)^{\otimes n_w}, \quad \mathcal{A} = (\mathbb{C}^2)^{\otimes n_a},$$

  and the functions $n_w, n_a : \mathbb{N} \to \mathbb{N}$ grow at most polynomially in $|x|$
- *V consists of $s(|x|)$ elementary gates where the function $s : \mathbb{N} \to \mathbb{N}$ grows at most polynomially in $|x|$*
- *if $x \in L$ (YES case) then there exists a witness state $|\psi\rangle \in \mathcal{W}$ such that*

  $$\|PV|\psi\rangle|\mathbf{0}\rangle\|^2 \geq a \tag{6}$$

- *if $x \notin L$ (NO case) then for all states $|\psi\rangle \in \mathcal{W}$ we have that*

  $$\|PV|\psi\rangle|\mathbf{0}\rangle\|^2 \leq b \tag{7}$$

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

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

Remark 2.5. 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 polylog$(1/\varepsilon)$ and increasing n_a by polylog$(1/\varepsilon)$ qubits, with no change in n_w [25, 26].

3 Quantum non-expander is in QMA

We now show that the problem defined in Definition 2.3 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

$$\|\Phi(A)\|_F > \alpha\|A\|_F. \tag{8}$$

We may assume w.l.o.g. 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:

$$\|A\|_F^2 = \langle\psi_A|\psi_A\rangle,$$

$$\mathrm{Tr}[A] = \sqrt{N}\langle\varphi|\psi_A\rangle,$$

where $|\varphi\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N}|i\rangle \otimes |i\rangle$, and

$$\|\Phi(A)\|_F^2 = \langle\psi_A|W^\dagger W|\psi_A\rangle,$$

where

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

and $\overline{U}_d$ denotes the complex conjugate of U_d.

First, to check whether $\mathrm{Tr}[A] = 0$, 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 $d, e = 1, \ldots, D$, define the unitaries

$$V_{d,e} = (U_d^\dagger \otimes U_d^T)(U_e \otimes \overline{U}_e).$$

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

$$\langle\psi_A|W^\dagger W|\psi_A\rangle = \frac{1}{D^2}\sum_{d,e}\langle\psi_A|V_{d,e}|\psi_A\rangle = \frac{1}{D} + \frac{2}{D^2}\sum_{d<e}\mathrm{Re}\langle\psi_A|V_{d,e}|\psi_A\rangle.$$

Arthur can estimate the values $\mathrm{Re}\langle\psi_A|V_{d,e}|\psi_A\rangle$ using the Hadamard test [shown in Fig. (1)] since it will output 0 with probability $\Pr(0) = \frac{1}{2}(1 + \mathrm{Re}\langle\psi_A|V_{d,e}|\psi_A\rangle)$. From this Arthur can calculate $\langle\psi_A|W^\dagger W|\psi_A\rangle = \|\Phi(A)\|_F^2$ and ensure it exceeds α^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

$$\langle\psi_A|W^\dagger W|\psi_A\rangle = \|\Phi(A)\|_F^2 \leqslant \beta^2.$$

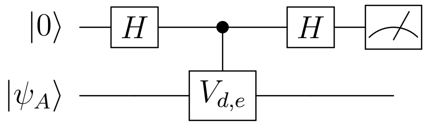

Figure 1: Hadamard test for $V_{d,e}$

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

As in the original definition of QMA in [24], 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 [25], we can transform a quantum circuit requiring $|\psi\rangle^{\otimes k}$ into one that requires only a single copy of $|\psi\rangle$.

4 Some technical tools

4.1 The Frobenius norm

In the proof that quantum non-expander 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

$$\|B\|_F = \sqrt{\mathrm{Tr}[B^\dagger B]} = \sqrt{\sum_{ij} |b_{ij}|^2}. \tag{9}$$

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

$$\Big\| \, |\psi\rangle\langle\phi| \, \Big\|_F = \sqrt{\langle\psi|\psi\rangle \, \langle\phi|\phi\rangle} = \Big\||\psi\rangle\Big\|\Big\||\phi\rangle\Big\|. \tag{10}$$

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

In this paper we denote the Pauli matrices on one qubit by σ_i, with $\sigma_0 = \mathbb{1}$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, 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 σ_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 σ_i are traceless for $i = 1, 2, 3$, the traceless condition on A therefore becomes $\mathrm{Tr}[A_0] = 0$. 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

$$\left\| \sum_{\mathrm{i}=0}^{3} \mathrm{A_i} \otimes \sigma_{\mathrm{i}} \right\|_F \geqslant \sqrt{2}\, \|A_0\|_F \,. \tag{11}$$

A quantum operation G is called a pinching operator if $G(B) = \sum_P PBP$ where P are non-overlapping projectors with $\sum_P P = \mathbb{1}$. Pinching operators are trace preserving,

$$\mathrm{Tr}\left[\sum_P PBP\right] = \mathrm{Tr}[B]\,, \tag{12}$$

and moreover, (by the pinching inequality) cannot increase Frobenius norm:

$$\left\| \sum_P PBP \right\|_F \leqslant \|B\|_F \,. \tag{13}$$

It should be noted that a quantum expander $\mathcal{E}$ is also norm-non-increasing,

$$\|\mathcal{E}(B)\|_F \leqslant \|B\|_F \,, \tag{14}$$

and similarly for any projector P,

$$\|PBP\|_F \leqslant \|B\|_F \,. \tag{15}$$

4.2 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 ΛU to indicate a controlled-U operation.

Definition 4.1 (Controlled expander). *Let $\mathcal{F}$ be a quantum expander with operation elements $\{U_i : i = 1 \dots m\}$ so that $\mathcal{F}(B) = \frac{1}{m}\sum_{i=1}^m U_i B U_i^\dagger$. The controlled expander $\Lambda\mathcal{F}$ is defined to be the m-regular superoperator whose operation elements are the controlled unitaries $\{\Lambda U_i : i = 1 \dots m\}$.*

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

$$\begin{aligned}
\Lambda\mathcal{F}\,(A \otimes B) &= \frac{1}{m}\sum_{i=1}^{m}\Big[(\Lambda U_i)(A \otimes B)(\Lambda U_i^\dagger)\Big] \\
&= \frac{1}{m}\sum_{i=1}^{m}\Big[(P \otimes U_i + Q \otimes \mathbb{1})(A \otimes B)(P \otimes U_i^\dagger + Q \otimes \mathbb{1})\Big] \\
&= \frac{1}{m}\sum_{i=1}^{m}\Big[PAP \otimes U_i B U_i^\dagger + PAQ \otimes U_i B + QAP \otimes B U_i^\dagger + QAQ \otimes B\Big] \\
&= PAP \otimes \frac{1}{m}\sum_i (U_i B U_i^\dagger) + PAQ \otimes \left(\frac{1}{m}\sum_i U_i\right) B \qquad (16) \\
&\qquad + QAP \otimes B\left(\frac{1}{m}\sum_i U_i^\dagger\right) + QAQ \otimes B.
\end{aligned}$$

Note that if we impose on $\mathcal{F}$ the requirement that

$$\sum_i U_i = 0 \qquad (17)$$

then we obtain

$$\Lambda\mathcal{F}\,(A \otimes B) = PAP \otimes \mathcal{F}(B) + QAQ \otimes B \qquad (18)$$

which is how we would naturally desire a controlled expander to act. Unfortunately, unlike Eq. (18), Eq. (16) has additional crossterms 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 $\mathcal{F}$ 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 $\mathcal{F}$; the expander $\mathcal{F}(B) = \frac{1}{m}\sum(U_i\ B\ U_i^\dagger)$ is invariant under $U_i \leftrightarrow -U_i$, even though the controlled expander $\Lambda\mathcal{F}(B) = \frac{1}{m}\sum(\Lambda U_i\ B\ \Lambda U_i^\dagger)$ 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 crossterms; 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 $\{\mathbb{1}, X, Y, Z\}$ with uniform probability 1/4. To ensure that Eq. (17) is satisfied, we therefore define the effect of $\mathcal{D}$ on a matrix σ to be

$$\mathcal{D}(\sigma) = \frac{1}{8}\sum_W W\sigma W = \mathbb{1}\,\frac{\mathrm{Tr}[\sigma]}{2}$$

where the sum is over $W \in \{\mathbb{1}, X, Y, Z, -\mathbb{1}, -X, -Y, -Z\}$. Consequently, the controlled complete depolarizer $\Lambda\,\mathcal{D}$ with a single qubit target and (possibly multiqubit)

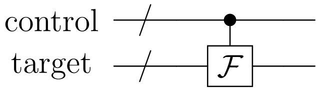

Figure 2: A controlled expander, $\Lambda\mathcal{F}$

control projectors P (indicating apply $\mathcal{D}$) and Q (indicating do nothing) is the 8-regular superoperator with operation elements

$$\{\Lambda(\mathbb{1}), \Lambda(X), \Lambda(Y), \Lambda(Z), \Lambda(-\mathbb{1}), \Lambda(-X), \Lambda(-Y), \Lambda(-Z)\}$$

having the effect

$$\Lambda\,\mathcal{D}(A \otimes \sigma) = PAP \otimes \mathbb{1}\frac{\mathrm{Tr}[\sigma]}{2} + QAQ \otimes \sigma. \tag{19}$$

Although controlled expanders are not actually quantum gates, we will nevertheless include them in circuit diagrams. If $\Lambda\mathcal{F}(B) = \frac{1}{m}\sum_i(\Lambda U_i \; B \; \Lambda U_i^\dagger)$ 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 (firstly, because depending on the control qubit, the operator might not do anything at all, and secondly 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 $\Lambda\,\mathcal{D}$, thus indicating that $\Lambda\,\mathcal{D}$ is not a good expander.

5 Quantum non-expander is QMA-hard

5.1 Outline of the proof

Let L be any language in $\mathrm{QMA}(\frac{2}{3}, \frac{1}{3})$. We show that the quantum non-expander problem is QMA-hard by reducing L to a quantum non-expander problem. Specifically, let x be an $|x|$-bit problem instance whose inclusion in L, or lack-thereof, we wish to determine. Because $L \in \mathrm{QMA}$ we have access to a verifier circuit satisfying Eqs. (6) and (7) acting on a witness space of $n_w = \mathrm{poly}(|x|)$ qubits and some ancilla space. For reasons that will become apparent later, we now use QMA amplification to give that $L \in \mathrm{QMA}(a, b)$ for polynomially separated a and b where

$$a > 0.99 \quad \text{and} \quad b < (0.1)2^{-(n_w+1)}.$$

Note from Remark 2.5 that this can be done without increasing the size of the witness space of the verifier. Let the resulting $\mathrm{QMA}(a, b)$ verifier circuit be called V, which acts on the same witness space of $n_w = \mathrm{poly}(|x|)$ qubits and some ancilla space of $n_a = \mathrm{poly}(|x|)$ ancilla qubits. Merlin can provide Arthur a valid (with high probability) witness if and only if $x \in L$.

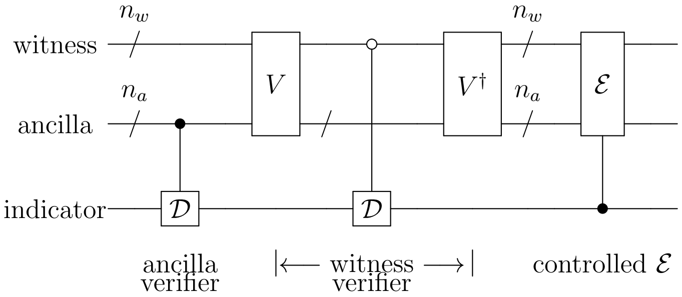

Figure 3: The map Φ constructed from the verifier circuit V, the complete depolarizer $\mathcal{D}$, and the $\kappa_{\mathcal{E}}$-contractive expander $\mathcal{E}$. The first controlled depolarizer is applied only if the ancillae are not all zero and the second one only if the top output is zero. The controlled $\mathcal{E}$-expander is applied only if the bottom qubit is one. Note that this figure is not a true circuit because $\mathcal{D}$ and $\mathcal{E}$ are quantum expanders, not unitary gates.

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 A.2 using Ref [6]. Using V and $\mathcal{E}$, we create a quantum expander Φ that is bad if $x \in L$ but good if $x \notin L$; indeed, we will present polynomially-separated (in fact, constant) α and β such that Φ is a β-contracting expander if $x \notin L$ but is not an α-contracting expander if $x \in L$. The circuit for Φ is shown in Fig. 3, which we now describe in detail.

The map Φ 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 *indicator 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 $\Lambda_{anc}\mathcal{D}$, which applies the complete depolarizer $\mathcal{D}$ to the indicator qubit register only if

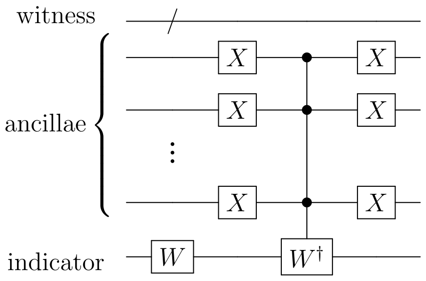

Figure 4: The controlled expander verifying the ancillae. The unitary W is selected from $\{\mathbb{1}, X, Y, Z, -\mathbb{1}, -X, -Y, -Z\}$ uniformly at random.

any of the ancilla bits are 1 (i.e. if they are not all 0). More technically, it is

$$\Lambda_{anc}\, \mathcal{D}(B) = \frac{1}{8} \sum_{W} \Lambda_{anc} W \ B \ \Lambda_{anc} W^\dagger$$

(with $W \in \{\mathbb{1}, X, Y, Z, -\mathbb{1}, -X, -Y, -Z\}$), where $\Lambda_{anc} W$ is the gate shown in Fig. 4. Note that $\Lambda_{anc} W$ requires a controlled-$W^\dagger$ gate controlled by n_a qubits, which can be implemented with ${n_a}^2$ gates using no extra work qubits [2]. (It is important that the implementation not require work qubits, because we demand that there are 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 on $n_w + n_a - 1$ 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 gate, which is the controlled expander $\Lambda_{ind}\, \mathcal{E}$, acts, conditioned on whether the indicator qubit is $|1\rangle$. Intuitively, if the input was $|\psi\rangle \otimes |\mathbf{0}\rangle \otimes |0\rangle$, with the indicator qubit initialized to $|0\rangle$, with the ancilla qubits initialized to $|\mathbf{0}\rangle = |00\ldots0\rangle$, 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 $\frac{1}{2}\mathbb{1} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, then $\mathcal{E}$ will act on the top registers, resulting in a highly mixed output (across all three registers).

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

5.2 Analysis of NO case

First, consider the case in which $x \notin L$. We wish to show that Φ 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 $\sum_{\mathrm{i}=0}^{3} \mathrm{A_i} \otimes \sigma_{\mathrm{i}}$ for some matrices A_i with $\mathrm{Tr}[A_0] = 0$, where σ_i are the Pauli matrices on the indicator qubit register.

Both the witness and ancilla verifiers are controlled depolarizers, and we can analyse 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 $Q_a = |00\ldots0\rangle\langle00\ldots0|_{anc}$ (more properly written as $Q_a = \mathbb{1}_{\mathrm{wit}} \otimes |00\ldots0\rangle\langle00\ldots0|_{anc} \otimes \mathbb{1}_{ind}$) and $P_a = \mathbb{1} - Q_a = \sum_{x\neq00\ldots0} |x\rangle\langle x|_{anc}$. For the witness verifier, $Q_w = V^\dagger\,|1\rangle\langle1|_{top} V$ and $P_w = V^\dagger\,|0\rangle\langle0|_{top} V$ (so that $P_w + Q_w = \mathbb{1}$). Here the subscript *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

$$\begin{aligned} F\left(\sum_{i=0}^{3} A_i \otimes \sigma_i\right) &= \sum_{i=0}^{3} \left[PA_iP \otimes \mathbb{1}\frac{\mathrm{Tr}[\sigma_i]}{2} + QA_iQ \otimes \sigma_i \right] \\ &= PA_0P \otimes \mathbb{1} + \sum_{i=0}^{3} QA_iQ \otimes \sigma_i. \end{aligned}$$

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

$$\begin{aligned} & F_w \circ F_a \left(\sum_{i=0}^{3} A_i \otimes \sigma_i\right) \\ = \;& F_w\left(P_aA_0P_a \otimes \mathbb{1}\right) + F_w\left(\sum_{i=0}^{3} Q_aA_iQ_a \otimes \sigma_i\right) \\ = \;& \left(P_wP_aA_0P_aP_w + Q_wP_aA_0P_aQ_w + P_wQ_aA_0Q_aP_w\right) \otimes \mathbb{1} + \sum_{i=0}^{3} Q_wQ_aA_iQ_aQ_w \otimes \sigma_i \\ = \;& \sum_{P} PA_0P^\dagger \otimes \mathbb{1} + \sum_{i=1}^{3} QA_iQ^\dagger \otimes \sigma_i, \end{aligned}$$

where the first sum is over $P \in \{P_wP_a, P_wQ_a, Q_wP_a, Q_wQ_a\}$ and where Q is the single product $Q = Q_wQ_a$ and $Q^\dagger = Q_aQ_w$. Notice that the $i = 0$ term (involving $\sigma_0 = \mathbb{1}$)

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

$$F_w \circ F_a \left(\sum_{i=0}^{3} A_i \otimes \sigma_i \right) = C(A_0) \otimes \mathbb{1} + \sum_{i=1}^{3} Q A_i Q^\dagger \otimes \sigma_i \tag{20}$$

where

$$C(A_0) = \sum_P P A_0 P^\dagger = \sum_{R_w = P_w, Q_w} R_w \left(\sum_{R_a = P_a, Q_a} R_a A_0 R_a \right) R_w = (G_w \circ G_a)(A_0)$$

is the composition of the pinching operators $G_j(B) = P_j B P_j + Q_j B Q_j$ applied to A_0.

Since C is the composition of pinching operators, Eqs. (12) and (13), along with Eq. (11), tell us

$$\mathrm{Tr}[C(A_0)] = \mathrm{Tr}[A_0] = 0 \tag{21}$$

and

$$\|C(A_0)\|_F \leqslant \|A_0\|_F \leqslant \frac{1}{\sqrt{2}} \left\| \sum_i A_i \otimes \sigma_i \right\|_F . \tag{22}$$

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

$$\Lambda\, \mathcal{E}\, (B \otimes b) = \mathcal{E}(B) \otimes |1\rangle\langle 1|\, b\, |1\rangle\langle 1| + B \otimes |0\rangle\langle 0|\, b\, |0\rangle\langle 0| .$$

Applying this to the state Eq. (20) we conclude that the effect of the map in Fig. 3 on the initial traceless matrix $\sum_{\mathrm{i}=0}^{3} \mathrm{A_i} \otimes \sigma_{\mathrm{i}}$ is

$$\Phi \left(\sum_{\mathrm{i}=0}^{3} \mathrm{A_i} \otimes \sigma_{\mathrm{i}} \right) = C(A_0) \otimes |0\rangle\langle 0| + \mathcal{E}\left(C(A_0)\right) \otimes |1\rangle\langle 1| + Q A_3 Q^\dagger \otimes |0\rangle\langle 0| - \mathcal{E}(Q A_3 Q^\dagger) \otimes |1\rangle\langle 1| .$$

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

$$\|\mathcal{E}\left(C(A_0)\right)\|_F \leqslant \kappa_{\mathcal{E}} \|C(A_0)\|_F . \tag{23}$$

Applying the triangle inequality and Eqs. (23), (14), and (22), we therefore have

$$\begin{aligned} \left\| \Phi \left(\sum_{\mathrm{i}=0}^{3} \mathrm{A_i} \otimes \sigma_{\mathrm{i}} \right) \right\|_F &\leqslant \|C(A_0)\|_F + \|\mathcal{E}\left(C(A_0)\right)\|_F + \left\| Q A_3 Q^\dagger \right\|_F + \left\| \mathcal{E}(Q A_3 Q^\dagger) \right\|_F \\ &\leqslant (1 + \kappa_{\mathcal{E}}) \|C(A_0)\|_F + 2 \left\| Q A_3 Q^\dagger \right\|_F \\ &\leqslant \frac{1 + \kappa_{\mathcal{E}}}{\sqrt{2}} \left\| \sum_{\mathrm{i}=0}^{3} \mathrm{A_i} \otimes \sigma_{\mathrm{i}} \right\|_F + 2 \left\| Q A_3 Q^\dagger \right\|_F . \end{aligned} \tag{24}$$

Note that we cannot make a claim similar to Eq. (23) for $\mathcal{E}(QA_3Q^\dagger)$ because $QA_3Q^\dagger$ 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 $QA_3Q^\dagger$ vanishes and we are done. In QMA(a,b), however, we must upper bound $\left\|QA_3Q^\dagger\right\|_F$, which we now proceed to do.

Because $x \notin L \in$ QMA(a,b) we are assured that for any purported witness $|\psi\rangle$,

$$\|Q_w|\psi\rangle|\mathbf{0}\rangle\| \leqslant \sqrt{b}. \tag{25}$$

Because Q_a projects onto the $|\mathbf{0}\rangle\langle\mathbf{0}|$ ancilla subspace, we may write

$$Q_aA_3Q_a = \sum_{\psi_1,\psi_2} c(\psi_1,\psi_2)\,|\psi_1\rangle\langle\psi_2| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|$$

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),

$$\begin{aligned}\left\|QA_3Q^\dagger\right\|_F &= \left\|\sum_{\psi_1,\psi_2} c(\psi_1,\psi_2)Q_w|\psi_1\rangle|\mathbf{0}\rangle\langle\psi_2|\langle\mathbf{0}|Q_w\right\|_F \\ &\leqslant \sum_{\psi_1,\psi_2} |c(\psi_1,\psi_2)|\left\|Q_w|\psi_1\rangle|\mathbf{0}\rangle\langle\psi_2|\langle\mathbf{0}|Q_w\right\|_F \\ &= \sum_{\psi_1,\psi_2} |c(\psi_1,\psi_2)|\left\|Q_w|\psi_1\rangle|\mathbf{0}\rangle\right\|_F\left\|Q_w|\psi_2\rangle|\mathbf{0}\rangle\right\|_F \\ &\leqslant \sum_{\psi_1,\psi_2} |c(\psi_1,\psi_2)|\,b.\end{aligned}$$

The matrix c has $(2^{n_w})^2$ elements, so its 1-norm and 2-norm are related by

$$\sum_{\psi_1,\psi_2} |c(\psi_1,\psi_2)| \leqslant 2^{n_w}\sqrt{\sum_{\psi_1,\psi_2} |c(\psi_1,\psi_2)|^2} = 2^{n_w}\left\|Q_aA_3Q_a^\dagger\right\|_F.$$

But by Eqs. (15) and (11), $\left\|Q_aA_3Q_a^\dagger\right\|_F \leqslant \|A_3\|_F \leqslant \frac{1}{\sqrt{2}}\left\|\sum_{\mathrm{i}=0}^3 \mathrm{A_i}\otimes\sigma_\mathrm{i}\right\|_F$; thus we conclude,

$$\left\|QA_3Q^\dagger\right\|_F \leqslant \frac{2^{n_w}}{\sqrt{2}}\left\|\sum_{\mathrm{i}=0}^3 \mathrm{A_i}\otimes\sigma_\mathrm{i}\right\|_F b. \tag{26}$$

Although 2^{n_w} is exponential in n_w, recall that b was chosen so that $2^{n_w+1}b \leqslant 0.1$. We conclude from Eqs. (24) and (26) that Φ is a β-contractive expander,

$$\left\|\Phi\left(\sum_{\mathrm{i}=0}^3 \mathrm{A_i}\otimes\sigma_\mathrm{i}\right)\right\|_F \leqslant \beta\left\|\sum_{\mathrm{i}=0}^3 \mathrm{A_i}\otimes\sigma_\mathrm{i}\right\|_F, \tag{27}$$

with

$$\beta = \frac{1+\kappa_{\mathcal{E}}+2^{n_w+1}b}{\sqrt{2}} < 0.85. \tag{28}$$

5.3 Analysis of YES case

Now consider the case in which $x \in L$. Since $L \in \mathrm{QMA}(a,b)$ there exists a valid witness $|\psi\rangle$ such that

$$\|Q_w|\psi\rangle|\mathbf{0}\rangle\|^2 \geqslant a. \tag{29}$$

From this witness we construct the density matrix $\Psi = |\psi\rangle\langle\psi|\otimes|\mathbf{0}\rangle\langle\mathbf{0}|\otimes|0\rangle\langle 0|$. Because Ψ passes the ancilla verifier unchanged and the witness verifier with very little change, Ψ is almost a fixed point of our expander Φ (and indeed, for $\mathrm{QMA}(1,0)$ it is a fixed point); intuitively, therefore, Φ is a poor expander. The matrix $\tilde{I} = \frac{1}{2^{n_w+n_a+1}}\,\mathbb{1}$ is certainly a fixed point (for any unital map); therefore the traceless matrix

$$A = \Psi - \tilde{I} = |\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}| \otimes |0\rangle\langle 0| - \frac{1}{2^{n_w+n_a+1}}\,\mathbb{1}$$

is also expected to change very little under Φ. By showing this to be the case, we will show that Φ is not an α-contractive expander for an α that is polynomially separated from the β 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 Ψ is

$$\begin{aligned}
\Psi \quad &= \quad |\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}| \otimes |0\rangle\langle 0| \\
&\xrightarrow{\text{Ancilla verifier}} \quad |\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}| \otimes |0\rangle\langle 0| \\
&\xrightarrow{\text{Witness verifier}} \quad P_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)P_w \otimes \frac{\mathbb{1}}{2} + Q_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)Q_w \otimes |0\rangle\langle 0| \\
&\xrightarrow{\text{Controlled } \mathcal{E}} \quad \frac{1}{2}\,\mathcal{E}\left[P_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)P_w\right] \otimes |1\rangle\langle 1| \\
&\qquad + \frac{1}{2}P_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)P_w \otimes |0\rangle\langle 0| \\
&\qquad + Q_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)Q_w \otimes |0\rangle\langle 0|\,.
\end{aligned}$$

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

$$\begin{aligned}
\|\Phi(\Psi)\|_F^2 \quad &= \quad \frac{1}{4}\left\|\mathcal{E}\left[P_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)P_w\right]\right\|_F^2 \\
&\qquad + \frac{1}{4}\left\|P_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)P_w\right\|_F^2 \\
&\qquad + \left\|Q_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)Q_w\right\|_F^2 \\
&\geqslant \quad \left\|Q_w\big(\,|\psi\rangle\langle\psi| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|\,\big)Q_w\right\|_F^2 \\
&= \quad \|Q_w|\psi\rangle|\mathbf{0}\rangle\|^4 \\
&\geqslant \quad a^2
\end{aligned} \tag{30}$$

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

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

$$\|A\|_F^2 = 1 - \frac{1}{2^{n_w+n_a+1}}. \tag{31}$$

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

$$\begin{aligned}
\|\Phi(A)\|_F^2 &= \left\|\Phi(\Psi) - \Phi(\tilde{I})\right\|_F^2 \\
&= \mathrm{Tr}\left[\Phi(\Psi)^\dagger \Phi(\Psi)\right] + \mathrm{Tr}\left[\tilde{I}^2\right] - \mathrm{Tr}\left[\Phi(\Psi)\tilde{I}\right] - \mathrm{Tr}\left[\Phi(\Psi)^\dagger \tilde{I}\right] \\
&= \|\Phi(\Psi)\|_F^2 + \mathrm{Tr}\left[\tilde{I}^2\right] - 2\mathrm{Tr}\left[\Psi\tilde{I}\right] \\
&\geqslant a^2 - \frac{1}{2^{n_w+n_a+1}} \\
&= \|A\|_F^2 - (1-a^2) \\
&> \left[1 - \frac{8}{5}(1-a^2)\right] \|A\|_F^2
\end{aligned}$$

where in the last inequality we have used from Eq. (31) that for $n_w \geqslant 1$ we have $\frac{5}{8} < \|A\|_F^2 \leqslant 1$. Thus we conclude that Φ is not an α-contractive expander,

$$\|\Phi(A)\|_F > \alpha \|A\|_F , \tag{32}$$

with

$$\alpha = \sqrt{1 - \frac{8}{5}(1-a^2)} > 0.98. \tag{33}$$

Note that α and β are constants, and therefore certainly polynomially separated.

6 Conclusion

We have presented a new computational problem, *quantum non-expander*, 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 non-expander problem.

Acknowledgments

This work was supported in part by the U.S. Department of Energy under cooperative research agreement Contract Number DE-FG02-05ER41360, as well as by the National Science Foundation Science and Technology Center for Science of Information under grant CCF-0939370. P.W. gratefully acknowledges the support from the NSF CAREER Award CCF-0746600.

Contributions to this work by NIST, an agency of the US government, are not subject to copyright laws.

A Appendix

A.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), (3) and (4). We follow the arguments of sections 3.3 and 3.4 in [9].

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

$$A_{\alpha\sigma} = \frac{1}{\sqrt{2}}(-i)^{\sigma}(U_\alpha + (-1)^{\sigma} U_\alpha^\dagger), \qquad B_{\alpha\sigma} = \frac{1}{\sqrt{2}} i^{\sigma}(f_\alpha + (-1)^{\sigma} f_\alpha^\dagger).$$

Then we can write the interaction Hamiltonian in the form

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

This form is convenient because $A_{\alpha\sigma}$ and $B_{\alpha\sigma}$ are Hermitian.

In the weak-coupling limit ($\varepsilon \to 0$), one gets the following master equation (equation 3.140 in [9], simplified using the fact that $H_S = 0$):

$$\frac{d}{dt}\rho_S(t) = -i[H_{LS}, \rho_S(t)] + \mathcal{D}(\rho_S(t)), \tag{34}$$

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

$$H_{LS} = \sum_{\alpha\beta\sigma\tau} S_{\alpha\beta\sigma\tau} A_{\alpha\sigma}^\dagger A_{\beta\tau}, \qquad \mathcal{D}(\rho_S) = \sum_{\alpha\beta\sigma\tau} \gamma_{\alpha\beta\sigma\tau} \Big(A_{\beta\tau} \rho_S A_{\alpha\sigma}^\dagger - \frac{1}{2}\{A_{\alpha\sigma}^\dagger A_{\beta\tau}, \rho_S\} \Big),$$

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

$$S_{\alpha\beta\sigma\tau} = \frac{1}{2i}(\Gamma_{\alpha\beta\sigma\tau} - \Gamma_{\beta\alpha\tau\sigma}^*), \qquad \gamma_{\alpha\beta\sigma\tau} = \Gamma_{\alpha\beta\sigma\tau} + \Gamma_{\beta\alpha\tau\sigma}^*,$$

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

$$\Gamma_{\alpha\beta\sigma\tau} = \int_0^\infty ds \langle B_{\alpha\sigma}^\dagger(s) B_{\beta\tau}(0)\rangle, \qquad B_{\alpha\sigma}(t) = e^{iH_B t} B_{\alpha\sigma} e^{-iH_B t}.$$

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

$$\begin{aligned}\langle B_{\alpha\sigma}^\dagger(s) B_{\beta\tau}(0)\rangle &= \frac{1}{2} i^{\sigma} i^{\tau} \frac{1}{|\Omega|} \sum_{kk'} \Big(e^{-is\omega_k} \langle b_{\alpha k} b_{\beta k'}\rangle + e^{-is\omega_k} (-1)^{\tau} \langle b_{\alpha k} b_{\beta k'}^\dagger\rangle \\ &\qquad + (-1)^{\sigma} e^{is\omega_k} \langle b_{\alpha k}^\dagger b_{\beta k'}\rangle + (-1)^{\sigma} e^{is\omega_k} (-1)^{\tau} \langle b_{\alpha k}^\dagger b_{\beta k'}^\dagger\rangle \Big) \\ &= \frac{1}{2} i^{\sigma} i^{\tau} \delta_{\alpha\beta} \frac{1}{|\Omega|} \sum_{k} \Big((-1)^{\sigma} e^{is\omega_k} N(\omega_k) + e^{-is\omega_k} (-1)^{\tau} (1 + N(\omega_k)) \Big),\end{aligned}$$

where $N(\omega_k) = \frac{1}{\exp(\omega_k/T)-1}$. We take a continuum limit, replacing the sum $\frac{1}{|\Omega|}\sum_k$ 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 $\Gamma_{\alpha\beta\sigma\tau}$:

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

We can simplify the above formula by exchanging the integrals and using the identity $\int_0^\infty ds e^{-ixs} = \pi\delta(x) - i \cdot PV(\frac{1}{x})$, where $\delta(x)$ is the Dirac distribution and $PV(\frac{1}{x})$ is the Cauchy principal value (equation 3.202 in [9]). We then get:

$$\begin{aligned}\Gamma_{\alpha\beta\sigma\tau} &= \frac{1}{2} i^\sigma i^\tau \delta_{\alpha\beta} \int_\Omega \Big((-1)^\sigma N(\omega_k) \int_0^\infty e^{is\omega_k} ds + (-1)^\tau (1 + N(\omega_k)) \int_0^\infty e^{-is\omega_k} ds \Big) dk \\ &= \frac{1}{2} i^\sigma i^\tau \delta_{\alpha\beta} \Big((-1)^\sigma \pi N(0) + (-1)^\sigma i \cdot PV \int_\Omega \frac{N(\omega_k)}{\omega_k} dk \\ &\qquad + (-1)^\tau \pi (1 + N(0)) - (-1)^\tau i \cdot PV \int_\Omega \frac{1 + N(\omega_k)}{\omega_k} dk \Big).\end{aligned}$$

In particular, $\Gamma_{\alpha\beta\sigma\tau}$ can be written in the form

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

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

We can now calculate the "Lamb shift" Hamiltonian H_{LS} as follows:

$$\begin{aligned}S_{\alpha\beta\sigma\tau} &= \frac{1}{2i} \cdot \frac{1}{2} i^\sigma i^\tau \delta_{\alpha\beta} \Big((-1)^\sigma (Q_0 - Q_0^*) + (-1)^\tau (Q_1 - Q_1^*) \Big), \\ H_{LS} &= \frac{Q_0 - Q_0^*}{4i} \sum_\alpha \Big(\sum_\sigma i^\sigma (-1)^\sigma A_{\alpha\sigma}^\dagger \Big) \Big(\sum_\tau i^\tau A_{\alpha\tau} \Big) \\ &\quad + \frac{Q_1 - Q_1^*}{4i} \sum_\alpha \Big(\sum_\sigma i^\sigma A_{\alpha\sigma}^\dagger \Big) \Big(\sum_\tau i^\tau (-1)^\tau A_{\alpha\tau} \Big) \\ &= \frac{Q_0 - Q_0^*}{4i} \sum_\alpha \sqrt{2} U_\alpha^\dagger U_\alpha \sqrt{2} + \frac{Q_1 - Q_1^*}{4i} \sum_\alpha \sqrt{2} U_\alpha U_\alpha^\dagger \sqrt{2} \\ &= \frac{Q_0 - Q_0^*}{2i} DI + \frac{Q_1 - Q_1^*}{2i} DI.\end{aligned}$$

So H_{LS} is a multiple of the identity, and it contributes nothing when we substitute it into the master equation (34).

Finally we can calculate the dissipator $\mathcal{D}$. First,

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

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

$$\mathcal{D}(\rho_S) = (Q_0 + Q_0^*) \sum_\alpha \Big(U_\alpha \rho_S U_\alpha^\dagger - \rho_S \Big) + (Q_1 + Q_1^*) \sum_\alpha \Big(U_\alpha^\dagger \rho_S U_\alpha - \rho_S \Big).$$

Note that $Q_0 + Q_0^*$ and $Q_1 + Q_1^*$ are positive real numbers. We substitute this into the master equation (34). This completes our proof of (5).

A.2 Controlled expanders

In this appendix, we outline how we obtain the requisite controlled expander $\Lambda\,\mathcal{E}$ needed for section 5. We use the results of Ben-Aroya, Schwartz, and Ta-Shma [6], whose Theorem 4.3 and 4.6 give the following result.

Theorem A.1. *There exists an integer D_0 such that for every $D > D_0$ and for every integer $t > 0$, there exists a explicit λ_t-contractive expander of degree D^2 on a space of dimension D^{8t} where $\lambda_t \leqslant \lambda + c\lambda^2$ with c a constant and $\lambda = \frac{4\sqrt{D-1}}{D}$.*

We will additionally use the following result, which follows directly from the definition. Here we use the notation that $\mathcal{F}^r$ denotes the r-fold composition of $\mathcal{F}$.

Proposition A.2. *If $\mathcal{F}$ is a λ-contractive expander of degree D on a space of size N, then for any positive integer r, $\mathcal{F}^r$ is a λ^r-contractive expander of degree D^r on a space of size N.*

In section 5 we require an $\kappa_{\mathcal{E}}$-contractive expander $\mathcal{E}$ with $\kappa_{\mathcal{E}} \leqslant 0.1$ on a space of size $N = 2^{n_w+n_a}$. Note that N is actually allowed to exceed $2^{n_w+n_a}$ since we can always have extra input ancillae that do nothing but are acted upon by the final controlled expander $\Lambda\,\mathcal{E}$.

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 $(\lambda+c\lambda^2)^r \leqslant 0.1$. Let $t = \left\lceil \frac{n_w+n_a}{8\log_2 D} \right\rceil = \frac{n_w+n_a+n_{extra}}{8\log_2 D}$ for some $n_{extra} < 8\log_2 D$.

Using the above theorem we are guaranteed the existance of a λ_t^r-contractive expander of degree D^{2r} on a space of size $D^{8t} = 2^{n_w+n_a+n_{extra}}$, where D and r are constants and $\lambda_t^r \leqslant 0.1$.

References

[1] D. Aharonov, D. Gottesman, S. Irani and J. Kempe, *The power of quantum systems on a line*, Communications in Mathematical Physics, 287(1), pp. 41–65, 2009.

[2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Phys. Rev. A 52, 3457, 1995.

[3] S. Beigi and P. W. Shor, *On the complexity of computing zero-error and Holevo capacity of quantum channels*, 2007; `http://arxiv.org/abs/0709.2090`

[4] A. Ben-Aroya and A. Ta-Shma, *Quantum expanders and the quantum entropy difference problem*, 2007; `http://arxiv.org/abs/quant-ph/0702129`

[5] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma, *An explicit construction of quantum expanders*, 2007; `http://arxiv.org/abs/0709.0911`

[6] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma, *Quantum expanders: motivation and construction*, Theory of Computing, vol. 6, pp. 47–79, 2010.

[7] A. D. Bookatz, *QMA-complete problems*, 2012; `http://arxiv.org/abs/1212.6312`

[8] F. Brandao, A. Harrow and M. Horodecki, *Local random quantum circuits are approximate polynomial-designs*, 2012; `http://arxiv.org/abs/1208.0692`

[9] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems*, Oxford University Press, 2002.

[10] O. Goldreich, *P, NP, and NP-completeness: the basics of complexity theory*, Cambridge University Press, 2010.

[11] D. Gross and J. Eisert, *Quantum Margulis expanders*, Quantum Inf. Comput., 8(8&9), pp. 722–733, 2008.

[12] A. W. Harrow, *Quantum expanders from any classical Cayley graph expander*, Quantum Inf. Comput., 8(8&9), pp. 715–721, 2008.

[13] M. Hastings, *Entropy and entanglement in quantum ground states*, Phys. Rev. B 76, 035114, 2007.

[14] M. B. Hastings, *Random unitaries give quantum expanders*, Phys. Rev. A, 76(3):032315, 2007.

[15] M. Hastings and A. Harrow, *Classical and quantum tensor product expanders*, Quantum Inf. Comput., 9(3&4):336360, 2009.

[16] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. 43, pp. 439–561, 2006.

[17] D. Janzing, P. Wocjan, and Th. Beth, *Non-identity check is QMA-complete*, International Journal of Quantum Information, 3(3), pp. 463–473, 2005.

[18] Z. Ji and X. Wu, *Non-identity check remains QMA-complete for short circuits*, Proc. Asian Conference on Quantum Information Science, 2009.

[19] J. Kempe, A. Kitaev, and O. Regev, *The complexity of the local Hamiltonian problem*, SIAM J. Comput., 35(5), pp. 10701097, 2006.

[20] E. Knill, *Quantum randomness and nondeterminism*, 1996; `http://arxiv.org/abs/quant-ph/9610012`

[21] Y.-K. Liu, *Consistency of local density matrices is QMA-complete*, Proc. 10th International Workshop on Randomization and Computation, RANDOM 2006, Lecture Notes in Computer Science 4110, pp. 438-449, 2006.

[22] Y.-K. Liu, M. Christandl, and F. Verstraete, *N-representability is QMA-complete*, Phys. Rev. Lett. 98, 110503, 2007.

[23] R. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics, 21(6&7), pp 467-488, 1982.

[24] A. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and quantum computation*, American Mathematical Society, 2002.

[25] C. Marriott and J. Watrous, *Quantum Arthur-Merlin games*, Computational Complexity, 14(2):122152 (2005).

[26] D. Nagaj, P. Wocjan, and Y. Zhang, *Fast amplification of QMA*, Quantum Information and Computation, 9(11&12), pp. 10531068, 2009.

[27] J. Watrous, *Succinct quantum proof for properties of finite groups*, Proc. 41st Foundations on Computer Science, pp. 537–546, 2000.