Quantum interactive proofs and the complexity of entanglement detection

Kevin Milner∗  Gus Gutoski†  Patrick Hayden∗  Mark M. Wilde‡

August 27, 2013

Abstract

This paper identifies a formal connection between physical problems related to entanglement detection and complexity classes in theoretical computer science. In particular, we show that to nearly every quantum interactive proof complexity class (including \(BQP\), \(QMA\), \(QMA(2)\), \(QSZK\), and \(QIP\)), there corresponds a natural entanglement or correlation detection problem that is complete for that class. In this sense, we can say that an entanglement or correlation detection problem captures the expressive power of each quantum interactive proof complexity class. The only promise problem of this flavor that is not known to be complete for a quantum interactive proof complexity class is a variation of the original quantum separability problem in which the goal is to decide if a quantum state output by a quantum circuit is separable or entangled. We also show that the difficulty of entanglement detection depends on whether the distance measure used is the trace distance or the one-way LOCC distance.

1 Introduction

Certain families of decision problems have proven to be particularly versatile and expressive in complexity theory, in the sense that slightly varying their formulation can tune the difficulty of the problems through a wide range of complexity classes. Adding quantifiers to the problem of evaluating a Boolean formula, for example, brings the venerable satisfiability problem up through the levels of the polynomial hierarchy [Sto76] all the way up to PSPACE [Sip96], at each level providing a decision problem complete for the associated complexity class. Moreover, adding limitations to the format of the Boolean satisfiability problem gives decision problems complete for a variety of more limited classes. Likewise, in the domain of interactive proofs [Bab85, GMR85, BM88, GMR89, Wat03, KW00, Wat09a], problems based on distinguishing probability distributions or quantum states, depending on the setting, arise very naturally.

In the domain of quantum information theory, quantum mechanical entanglement is responsible for many of the most surprising and, not coincidentally, useful potential applications of quantum

∗School of Computer Science, McGill University, Montreal, Quebec H3A 2A7, Canada
†Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada.
‡Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

1For example, it is known that if clauses of the Boolean satisfiability problem are limited to two variables each, the resulting problem (2SAT) is \(NL\)-complete [Pap94], while if one allows only Horn clauses the resulting problem (HORNSAT) is \(P\)-complete [CN10], and if one removes any such limitations on clauses the problem (SAT) is \(NP\)-complete [Coo71].
information [HHHH09], including quantum teleportation [BBC+93], super-dense coding [BW92], enhanced communication capacities [BSST99, BSST02, CLMW10], device-independent quantum key distribution [Eke91, VV12], and communication complexity [CB97]. Thus, deciding whether the correlations in a given state represent true quantum entanglement is a prominent and long-standing question that frequently resurfaces in different forms. The complexity of determining whether a given mixed quantum state is separable or entangled therefore arose early and was resolved: the problem is $\text{NP}$-complete with respect to Cook reductions when the state is specified as a density matrix and one demands an error tolerance no smaller than an inverse polynomial in the dimension of the matrix [Gur03, Gha10].

From a physics or engineering perspective, however, it is often more natural to specify a quantum state as arising from a sequence of specified operations or the application of a local Hamiltonian. This formulation of the quantum separability problem is more general and solving it is more difficult: it is known to be hard for the complexity class quantum statistical zero-knowledge ($\text{QSZK}$) as well as $\text{NP}$-hard with respect to Cook reductions, while lying inside the class $\text{QIP}(2)$ of promise problems decidable by a two-message quantum interactive proof system [HMW13].

In this paper we explore several variations on the complexity of determining whether or not a state specified by a quantum circuit is entangled. We vary, for example, whether we allow general mixed states or restrict to pure states. We also compare the difficulty of deciding whether entanglement is present (separable versus entangled states) with the difficulty of identifying any correlation whatsoever (product versus non-product states). One of the most subtle and interesting variations is to alter the metric used to measure distance between quantum states: we show that the complexity of detecting entanglement produced by an isometry is either $\text{QMA}(2)$-complete or $\text{QMA}$-complete according to whether one measures distance using the familiar trace distance or the more forgiving “one-way LOCC” distance of Ref. [MWW09].

We consider all problems in terms of general multipartite states, though only bipartite states are required for the hardness results—this indicates that in general, detecting multipartite entanglement or correlation may be no more difficult than the detection of bipartite entanglement or correlation. We also consider these problems for quantum channels, asking whether there exists an input to the channel with the specified properties. In most cases, the resulting problem proves to be complete for a complexity class of quantum interactive proofs, providing characterizations of $\text{BQP}$, $\text{QMA}$, $\text{QMA}(2)$, and $\text{QSZK}$ [Wat09a]. (We will define these classes below for those unfamiliar with them.)

## 2 Overview of Results

Figure 1 provides a concise summary of our results. Refer to this table for a brief description of the promise problems. Below we give more details of our results along with their relation to prior results in the literature:

- **QPROD-PURE-STATE** is complete for the class $\text{BQP}$ for any inverse polynomial gap in completeness and soundness parameters, as stated in Theorem 10. We demonstrate that this problem is in $\text{BQP}$ by employing the “product test” introduced in [MCKB05] along with the analysis of its success probability from [HM10]. We also provide a simple reduction of a general $\text{BQP}$ quantum circuit to the problem of pure-state entanglement detection.

- **QSEP-ISOMETRY$_{1,1}$-LOCC** is complete for the class $\text{QMA}$ for any inverse polynomial gap in completeness and soundness parameters. We show that this problem is in $\text{QMA}$ by building
| Problem               | Summary                                                                 | Complexity         | Circuit |
|----------------------|-------------------------------------------------------------------------|--------------------|---------|
| QPROD-PURE-STATE     | Is the state generated by the pure-state quantum circuit close to a product state? | BQP-complete       | ![Circuit](U) |
| QSEP-ISOMETRY$_{1,1}$-LOCC | Is there an input to the isometry such that the output is close to a separable state in the trace distance, or does every input lead to an output that is far from separable in 1-LOCC distance? | QMA-complete       | ![Circuit](U) |
| QPROD-ISOMETRY       | Is there an input to the isometry such that the output is close to a product/separable state? | QMA(2)-complete    |         |
| QSEP-ISOMETRY        | Is the state generated by the mixed-state circuit close to a product state? | QSZK-complete      | ![Circuit](U) |
| QPROD-STATE          | Is the state generated by the mixed-state circuit close to a product state? | In QIP(2), QSZK-hard, NP-hard |         |
| QSEP-STATE$_{1,1}$-LOCC | Is the state generated by the mixed-state circuit close to a separable state? |                     | ![Circuit](U) |
| QSEP-CHANNEL$_{1,1}$-LOCC | Is there an input to the channel such that the output is close to a separable state in trace distance or does every input lead to an output that is far from separable in 1-LOCC distance? | QIP-complete       | ![Circuit](U) |

Figure 1: The collected results of entanglement detection problems and their complexity. The leftmost column gives the name of the promise problem. Problem names subscripted with “1, 1-LOCC” indicate that the distance measure for yes-instances is the trace distance while the distance measure for no-instances is the one-way LOCC distance. The second column gives a question to which the problem corresponds. The third column states our complexity-theoretic characterization of the problem. The final column depicts a quantum circuit corresponding to the promise problems.
upon prior work of Brandão et al. [BCY11] and the notion of $k$-extendibility [Wer89a, DPS04]. (Some of us used a similar approach in previous work to place QSEP-STATE$_{1,1}$-LOCC in QIP(2) [HMW13].) The QMA proof system requires the prover to provide: 1) a quantum input to the isometry such that the output is close to some product state $|\psi\rangle_A \otimes |\phi\rangle_B$ and 2) $k$ copies of $|\phi\rangle_B$. The verifier then checks whether the prover is being honest by performing phase estimation over the symmetric group on all of the $B$ systems [Kit95] (also called the “permutation test” [BBD+97, KNY08]). This proof system extends naturally to the multipartite case as well. We prove QMA-hardness of QSEP-ISOMETRY$_{1,1}$-LOCC by reusing the BQP reduction technique mentioned above.

- QPROD-ISOMETRY and QSEP-ISOMETRY are complete for the class QMA(2) for any inverse polynomial gap in completeness and soundness parameters. We give a QMA(2) proof system in which the verifier performs the product test mentioned above, and we can employ the QMA(k)-amplification results of Harrow and Montanaro to reduce the completeness and soundness errors to become negligible [HM10]. We then show that these problems are QMA(2)-hard by reducing a general QMA(2) verifier circuit to one for which the output can be made product if and only if there exist two product inputs that would cause the verifier to accept the output of the original general QMA(2) circuit.

- QPROD-STATE is complete for the class QSZK for a wide range of completeness and soundness parameters. This problem differs from the BQP-complete problem QPROD-PURE-STATE in that it allows for a mixed-state quantum circuit to generate the state rather than a unitary circuit. We show that QPROD-STATE is in QSZK by specifying a statistical zero-knowledge proof system that decides it, and we show QSZK-hardness by giving a reduction from the QSZK-complete promise problem QUANTUM-STATE-DISTINGUISHABILITY [Wat02, Wat09b] to QPROD-STATE.

- QSEP-STATE$_{1,1}$-LOCC is in the class SQG—a class introduced in [GW05] and shown to be equal to PSPACE in [GW13]. Some of us have shown in prior work that QSEP-STATE$_{1,1}$-LOCC is in QIP(2) [HMW13], which is already known to be contained in SQG and is believed to be a strict subset of it. Thus, this new bound is not a complexity-theoretic improvement over prior work.

However, it is interesting that QSEP-STATE$_{1,1}$-LOCC can be decided by a very natural protocol with only a single message from the prover—a witness—provided that the verifier is granted the additional ability to query a second, competing prover in his effort to check the veracity of the first prover’s purported witness. By contrast, the two-message single-prover quantum interactive proof for QSEP-STATE$_{1,1}$-LOCC of Ref. [HMW13] depends critically upon the ability of the verifier to exchange two messages with the prover.

The contributions of the present paper along with those in [HMW13] give a variety of entanglement or correlation detection promise problems that are complete for BQP, QMA, QMA(2), QSZK, and QIP, along with a problem that is in QIP(2). The present paper is structured around this

---

2In [HMW13], the QSEP-STATE$_{1,1}$-LOCC problem was called QSEP-CIRCUIT, but we have changed the name here to create a uniform nomenclature.

3In particular, QIP(2) is trivially contained in QIP and is believed to be a strict subset of it. It is known that QIP is contained in SQG [GW05] and indeed both of these classes are equal to PSPACE [GW13].
hierarchy of correlation detection problems, beginning with preliminary concepts related to quantum information and the quantum interactive proof hierarchy. In the subsequent sections, we give detailed definitions and justify our aforementioned claims that these various entanglement and correlation detection problems are in one-to-one correspondence with $\text{BQP}$, $\text{QMA}$, $\text{QMA}(2)$ and $\text{QSZK}$. For completeness, Section 9 reviews the results presented in [HMW13]. In Section 10 we briefly mention how our various proof systems provide operational interpretations for several geometric measures of entanglement (see Refs. [WG03] [CAH13] and references therein). Finally, we conclude in Section 11 with a summary of our results and a discussion of directions for future research.

3 Preliminaries

In this section, we review concepts and complexity classes that will be used throughout the paper, though general background knowledge of both quantum information theory and quantum computational complexity theory is assumed. For more in depth overviews of these fields, consult [NC00] [Wil11] [Wil13] and [Wat09a] [Aar13], respectively.

3.1 Distance measures

A quantum state is a positive semidefinite, unit-trace operator (referred to as the density operator) acting on some Hilbert space $\mathcal{H}$. Let $D(\mathcal{H})$ denote the set of density operators acting on a Hilbert space $\mathcal{H}$.

One distance measure often used in quantum information theory to quantify the distance between quantum states is the trace distance, induced by the trace norm. The trace norm of an operator $A$ is $\|A\|_1 \equiv \text{Tr}\{\sqrt{A^\dagger A}\}$. The trace distance has an important operational interpretation as the bias in distinguishing two states $\rho$ and $\sigma$, each elements of $D(\mathcal{H})$, so that the maximum probability $p_{\text{succ}}$ of successfully discriminating them is given by

$$p_{\text{succ}} = \frac{1}{2} \left( 1 + \frac{1}{2} \|\rho - \sigma\|_1 \right).$$

A variational characterization of the trace distance is as follows:

$$\|\rho - \sigma\|_1 = 2 \max_{0 \leq \Lambda \leq I} \text{Tr}\{\Lambda(\rho - \sigma)\},$$

where the measurement $\{\Lambda, I - \Lambda\}$ that achieves this maximum is known as the Helstrom measurement [Hel69] [Hol72] [Hel76]. This also leads to the following useful inequality that holds for all $\Gamma$ such that $0 \leq \Gamma \leq I$:

$$\text{Tr}\{\Gamma\rho\} \geq \text{Tr}\{\Gamma\sigma\} - \|\rho - \sigma\|_1.$$  \hfill (1)

The quantum fidelity $F(\rho, \sigma)$ between two quantum states $\rho$ and $\sigma$ is another measure of distinguishability, defined as follows:

$$F(\rho, \sigma) \equiv \|\sqrt{\rho}\sqrt{\sigma}\|_1^2.$$  \hfill (2)

Uhlmann proved that the fidelity is the optimal squared overlap between any two purifications of $\rho$ and $\sigma$ [Uhl76]:

$$F(\rho, \sigma) = \max_{|\phi_\rho\rangle, |\phi_\sigma\rangle} |\langle \phi_\rho | \phi_\sigma \rangle|^2.$$
Uhlmann’s characterization gives the fidelity an operational interpretation as the optimal probability with which a purification of $\rho$ would pass a test for being a purification of $\sigma$. Since all purifications are related by unitary transformations acting on the purifying system, it follows that

$$F(\rho, \sigma) = \max_U |\langle \phi_\rho | (U \otimes I_H) |\phi_\sigma \rangle|^2$$  \hspace{1cm} (3)

for any fixed purifications $|\phi_\rho\rangle$ and $|\phi_\sigma\rangle$ of $\rho$ and $\sigma$, respectively. The equivalence between (2) and (3) is commonly known as Uhlmann’s theorem. The fidelity and trace distance for general states are related by the Fuchs-van-de-Graaf inequalities [FvdG99]:

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2} \| \rho - \sigma \|_1 \leq \sqrt{1 - F(\rho, \sigma)},$$  \hspace{1cm} (4)

with the following equality holding for pure states

$$\frac{1}{2} \| \psi - \phi \|_1 = \sqrt{1 - F(\psi, \phi)}.$$  \hspace{1cm} (5)

The final relevant distance measure that we require is based on the maximum distinguishability of two states when restricting to local operations and one-way classical communication between the systems of the two states. This distance measure is known as the one-way LOCC distance (1-LOCC), induced by a 1-LOCC norm [MWW09]:

$$\| \rho_{AB} - \sigma_{AB} \|_{1\text{-LOCC}} \equiv \max_{\Lambda_{B \rightarrow X}} \| (I_A \otimes \Lambda_{B \rightarrow X}) (\rho_{AB} - \sigma_{AB}) \|_1,$$

for two bipartite states $\rho_{AB}, \sigma_{AB} \in D(H_A \otimes H_B)$ and where the maximization on the RHS is over all quantum-to-classical channels

$$\Lambda_{B \rightarrow X} (\omega) \equiv \sum_{x \in X} \text{Tr} \{ \Lambda_{x} \omega \} |x\rangle \langle x|,$$

with $\Lambda_{x} \geq 0$ for all $x \in X$, $\sum_{x \in X} \Lambda_{x} = I$, and $\{ |x\rangle \}$ some orthonormal basis. (Note that we could also define the 1-LOCC distance with respect to measurement maps on the $A$ systems, which generally gives a different value). This distance is the natural distance measure in the setting of Bell experiments [Bel64] or quantum teleportation. It is also clear from the definitions that

$$\| \rho - \sigma \|_{1\text{-LOCC}} \leq \| \rho - \sigma \|_1,$$

because a 1-LOCC protocol to distinguish states cannot do any better than a general protocol.

The 1-LOCC distance measure has been extended to multipartite quantum states in [LWT12, BaC12, BaH13]. On an $l$-partite system, the $l$-partite 1-LOCC distance is given by

$$\| \rho_{A_1 \ldots A_l} - \sigma_{A_1 \ldots A_l} \|_{1\text{-LOCC}} \equiv \max_{\Lambda_{A_2, \ldots, A_l}} \| (I_{A_1} \otimes \Lambda_{A_2} \otimes \cdots \otimes \Lambda_{A_l}) (\rho_{A_1 \ldots A_l} - \sigma_{A_1 \ldots A_l}) \|_1,$$

where each of $\Lambda_{2, \ldots, l}$ are quantum-to-classical channels. The interpretation here is that the last $l-1$ parties each perform a local measurement on their system and communicate the results to the first party, who then does her best to distinguish the two states.
3.2 Separability and \( k \)-extendibility

A multipartite state \( \rho_{A_1 \cdots A_l} \in \mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_l} \) is said to be separable if it admits a decomposition of the following form:

\[
\rho_{A_1 \cdots A_l} = \sum_{y \in \mathcal{Y}} p_Y(y) \sigma^{1,y}_{A_1} \otimes \cdots \otimes \sigma^{l,y}_{A_l},
\]

for collections \( \{\sigma^{1,y}_{A_1}\}, \ldots, \{\sigma^{l,y}_{A_l}\} \) of quantum states and some probability distribution \( p_Y(y) \) over an alphabet \( \mathcal{Y} \) \cite{Wer89b}. By applying the spectral theorem to each density operator, we can always find a decomposition of any separable state in terms of pure product states:

\[
\rho_{A_1 \cdots A_l} = \sum_{z \in \mathcal{Z}} p_Z(z) \left| \psi^{1,z}_{A_1} \right\rangle \left\langle \psi^{1,z}_{A_1} \right| \otimes \cdots \otimes \left| \psi^{l,z}_{A_l} \right\rangle \left\langle \psi^{l,z}_{A_l} \right|.
\]

States which cannot be written in this form are entangled. Let \( \mathcal{S} \) denote the set of separable states. Throughout this work we refer to states in \( \mathcal{S} \) as states that are separable across all named systems unless a specific cut is indicated.

States of the form \( \sigma^{1}_{A_1} \otimes \cdots \otimes \sigma^{l}_{A_l} \) (such that the distribution \( p_Y(y) \) in (8) is degenerate) are known as product states. Let \( \mathcal{P} \) denote the set of product states. \( \mathcal{P} \) is not a convex set, and the convex closure of \( \mathcal{P} \) is the set \( \mathcal{S} \). Operationally, product states are those that are completely uncorrelated between systems and so can be prepared on systems in complete isolation, while separable states can be prepared by means of classical communication between the systems. Furthermore, the correlation exhibited in separable states may be simulated by classical systems in a non-locality, Bell-like test \cite{Wer89b}.

Separability has a close connection with the notion of \( k \)-extendibility. A bipartite state \( \rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B) \) is \( k \)-extendible \cite{Wer89a, DPS02, DPS04} if there exists a state \( \omega_{AB_1 \cdots B_k} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \cdots \otimes \mathcal{H}_{B_k}) \) such that

1. Each Hilbert space \( \mathcal{H}_{B_i} \) is isomorphic to \( \mathcal{H}_B \) for all \( i \in \{1, \ldots, k\} \).
2. The state \( \omega_{AB_1 \cdots B_k} \) is invariant under permutations of the systems \( B_1 \) through \( B_k \). That is,

\[
\forall \pi \in S_k : \omega_{AB_1 \cdots B_k} = (I_A \otimes W_{B_1 \cdots B_k}^\pi) \omega_{AB_1 \cdots B_k} (I_A \otimes W_{B_1 \cdots B_k}^\pi)^\dagger,
\]

where \( S_k \) is the symmetric group on \( k \) elements and \( W_{B_1 \cdots B_k}^\pi \) is a unitary transformation that implements the permutation \( \pi \) on the \( B \) systems.
3. The state \( \omega_{AB_1 \cdots B_k} \) is an extension of \( \rho_{AB} \):

\[
\rho_{AB} = \text{Tr}_{B_{2 \cdots k}} \{ \omega_{AB_1 \cdots B_k} \}.
\]

Let \( \mathcal{E}_k \) denote the set of \( k \)-extendible states. Every separable state is \( k \)-extendible for all \( k \geq 2 \), because the following state

\[
\sum_{x \in X} p_X(x) |\psi_x\rangle_A \otimes |\phi_x\rangle_{B_1} \otimes \cdots \otimes |\phi_x\rangle_{B_k}
\]

is a suitable \( k \)-extension of any separable state \( \sum_{x \in X} p_X(x) |\psi_x\rangle_A \otimes |\phi_x\rangle_{B} \). On the other hand, if a state is not separable, there always exists some \( k \) for which the state is not \( k \)-extendible,
and furthermore, for every \( l > k \), the state is also not \( l \)-extendible \[\text{DPS02, DPS04}\]. This forms a hierarchy of approximations to the set of separable states, becoming exact in the limit as \( k \to \infty \).

The bipartite notion of \( k \)-extendibility has been further expanded in \[\text{DPS05, BaH13}\] to multipartite states, which requires that every system is extendible according to the conditions above. Specifically, a multipartite state \( \rho_C \in D(H_{A_1} \otimes \cdots \otimes H_{A_l}) \) (we abbreviate the combined systems \( A_1 \cdots A_l \) as \( C \) for simplicity) is \( k \)-extendible if there exists a state \( \omega_{C_1 \cdots C_k} \in D(H_{C_1} \otimes \cdots \otimes H_{C_k}) \) such that

1. Each Hilbert space \( H_{C_{i,j}} \) is isomorphic to \( H_{A_j} \) for all \( i \in \{1, \ldots, k\} \) and \( j \in \{1, \ldots, l\} \), where the notation \( C_{i,j} \) refers to the \( j \)th subsystem of \( C_i \).
2. For all parties \( j \in \{1, \ldots, l\} \), the state \( \omega_{CC_2 \cdots C_k} \) is invariant under permutations of the systems \( C_{1,j} \) through \( C_{k,j} \). Note that there are \( l \cdot k! \) such permutations.
3. The state \( \omega_{CC_2 \cdots C_k} \) is an extension of \( \rho_C \):

\[
\rho_C = \text{Tr}_{C_2 \cdots C_k} \{ \omega_{CC_2 \cdots C_k} \}.
\]

The following lemma is essential for some of our quantum interactive proof systems and expands Theorem 2 of \[\text{BaH13}\] to establish a notion of approximate \( k \)-extendibility. The proof of Lemma 1 is straightforward and can be found in Appendix A.1.

**Lemma 1** Let \( \rho_{A_1 \cdots A_l} \) be \( \varepsilon \)-far in one-way LOCC distance from the set of fully separable states, for some \( \varepsilon > 0 \):

\[
\min_{\sigma_{A_1 \cdots A_l} \in S} \| \rho_{A_1 \cdots A_l} - \sigma_{A_1 \cdots A_l} \|_{\text{1-LOCC}} \geq \varepsilon.
\]

Then the state \( \rho_{A_1 \cdots A_l} \) is \( \delta \)-far in trace distance from the set of \( k \)-extendible states:

\[
\min_{\sigma_{A_1 \cdots A_l} \in E_k} \| \rho_{A_1 \cdots A_l} - \sigma_{A_1 \cdots A_l} \|_1 \geq \delta,
\]

for \( \delta < \varepsilon \) and where

\[
k = \left\lceil l + \frac{4l^2 \log |C|}{(\varepsilon - \delta)^2} \right\rceil.
\]

### 3.3 Quantum interactive proofs

We now formally introduce the quantum interactive proof complexity classes that are relevant to this work. Quantum interactive proof systems involve multiple parties who exchange quantum information: a verifier who has access to a computationally bounded quantum computer and one or more untrustworthy provers who have access to powerful quantum computers bounded only by the laws of quantum mechanics (these provers can perform any unitary operation). The verifier aims to decide whether one of two promises is true—he can receive help from the provers by exchanging quantum messages with them, but he must perform tests to make sure that the provers are not trying to fool him. \( \text{QMA}(2) \) and \( \text{SQG} \) are the only multi-prover quantum interactive proof complexity classes that we consider in this work. All others that we consider (\( \text{BQP}, \text{QMA}, \text{QIP}(2), \text{QIP}(3), \) and \( \text{QSZK} \)) have just one prover.
3.3.1 BQP

The least powerful class within the quantum interactive proof hierarchy consists of a verifier who does not exchange any quantum messages with a prover. Bounded error quantum polynomial time (BQP) includes all promise problems that can be decided by a quantum verifier in polynomial time, and it is the most natural quantum extension of BPP and P, the classical probabilistic and deterministic verifier regimes, respectively. (The term verifier is used for consistency with what follows. However, in this case, there is no proof being verified—the verifier is simply working on his own.)

Definition 2 (BQP) Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, and let $c, s : \mathbb{N} \rightarrow [0, 1]$ be polynomial-time computable functions such that the gap $c - s$ is at least an inverse polynomial in the input length. Then $A \in \text{BQP}(c,s)$ if there exists a polynomial-time generated family of circuits $U = \{U_n : n \in \mathbb{N}\}$ that satisfies the following properties:

1. Completeness: For all input strings $x \in A_{\text{yes}}$, the probability of acceptance is at least $c(|x|)$.
2. Soundness: For all input strings $x \in A_{\text{no}}$, the probability of acceptance is at most $s(|x|)$.

We define $\text{BQP} = \text{BQP}(2/3, 1/3)$, though note that one can amplify the gap between $c$ and $s$ such that they become exponentially close to their extremes by employing parallel repetition. Thus, $\text{BQP} = \text{BQP}(1 - 2^{-p(n)}, 2^{-p(n)})$ for any polynomial function $p(n)$.

3.3.2 QMA

Giving the verifier access to a quantum proof, also called a quantum witness state, seems to greatly expand the set of problems that the verifier can decide in polynomial time. This class is known as Quantum Merlin-Arthur (QMA) [Kit99, Wat00], after the analogous probabilistic verifier class, Merlin-Arthur (MA), in which a computationally bounded verifier (Arthur) wishes to solve a problem with the help of a computationally unbounded but potentially dishonest prover (Merlin). This class is the most natural fully quantum extension of the famous deterministic class NP.

Definition 3 (QMA) Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, and let $c, s : \mathbb{N} \rightarrow [0, 1]$ be polynomial-time computable functions such that the gap $c - s$ is at least an inverse polynomial in the input length. Then $A \in \text{QMA}(c,s)$ if there exists a polynomial-time generated family of circuits $U = \{U_n : n \in \mathbb{N}\}$ that satisfies the following properties:

1. Completeness: For all input strings $x \in A_{\text{yes}}$, there exists a witness state on a polynomial number of qubits such that the probability of acceptance is at least $c(|x|)$.
2. Soundness: For all input strings $x \in A_{\text{no}}$ and all witness states, the probability of acceptance is at most $s(|x|)$.

Note that it suffices for the prover to provide a pure quantum witness state rather than a mixed one. By a simple convexity argument, one can see that for every mixed quantum witness state there exists a pure quantum witness state which has an acceptance probability that is only larger than or equal to that for the mixed witness state.

It is conventional to define $\text{QMA} = \text{QMA}(2/3, 1/3)$, but note that, as in the case of BQP, one can amplify the gap between $c$ and $s$ such that they become exponentially close to their extremes.
and thus $QMA = QMA(1 - 2^{-p(n)}, 2^{-p(n)})$ for any polynomial function $p(n)$. To obtain this result, one can exploit the QMA amplification technique of Marriott and Watrous in [MW05] or the more recent fast amplification procedure of Nagaj et al. in [NWZ09].

### 3.3.3 $QMA(2)$

Although we organize the quantum interactive proof hierarchy according to the number of interactions between the prover and verifier, we can also consider a natural extension of $QMA$ in which the verifier has access to unentangled quantum proofs from multiple quantum provers. It is clear that entanglement is a powerful tool in quantum information, and the ways in which the prover can fool the verifier in $QMA$ are directly related to his ability to entangle the witness state. The class $QMA(k)$ consists of all promise problems that can be decided with the help of $k$ unentangled quantum witness states.

**Definition 4 ($QMA(k)$)** Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, and let $c, s : \mathbb{N} \rightarrow [0, 1]$ be polynomial-time computable functions such that the gap $c - s$ is at least an inverse polynomial in the input length. Then $A \in QMA(k, c, s)$ if there exists a polynomial-time generated family of circuits $U = \{U_n : n \in \mathbb{N}\}$ that satisfies the following properties:

1. **Completeness:** For all input strings $x \in A_{\text{yes}}$, there exist $k$ unentangled quantum witness states on a polynomial number of qubits each, such that the probability of acceptance is at least $c(|x|)$.

2. **Soundness:** For all input strings $x \in A_{\text{no}}$ and all possible witness states, the probability of acceptance is at most $s(|x|)$.

Note that allowing classical communication between the provers does not change this complexity class. Indeed, by coordinating with classical communication, they could prepare a separable state to send to the verifier. However, it suffices for the provers to provide a pure, product quantum witness state rather than a mixed separable state. Again, by a simple convexity argument and the decomposition in [9], one can see that for every separable quantum witness state there exists a pure product quantum witness state which has an acceptance probability that is only larger than or equal to that for the separable state. So classical communication does not help them to cheat.

This family of classes was originally defined in [KMY01]. We define $QMA(k) = QMA(k, 2/3, 1/3)$, though Harrow and Montanaro recently showed in [HM10] that $QMA(k) = QMA(2)$ for $k$ no larger than a polynomial in the input length, and further that $QMA(2) = QMA(2, 1 - 2^{-p(n)}, 2^{-p(n)})$ for any polynomial function $p(n)$. It remains unclear exactly how powerful $QMA(2)$ is in relation to the single-prover quantum interactive proof hierarchy, but there is evidence that the guarantee of unentangled proofs is a very powerful resource [ABD09]. Estimating the minimum energy of a sparse Hamiltonian over all bipartite product states is a non-trivial promise problem that is complete for $QMA(2)$ [CS12]. The present paper gives another non-trivial promise problem that is complete for $QMA(2)$.

### 3.3.4 $QIP(m)$

We now formally define the family of classes that constitute the quantum interactive proof hierarchy. The class $QIP(m)$ is defined as the class of problems that a verifier can decide if he is allowed to
exchange at most $m$ messages with the prover, and it is analogous to the class $\text{IP}(m)$ in the classical probabilistic verifier regime.

**Definition 5 (QIP)** Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, and let $c, s : \mathbb{N} \rightarrow [0, 1]$ be polynomial-time computable functions such that the gap $c - s$ is at least an inverse polynomial in the input length. Let $m$ be a positive integer no larger than a polynomial in the input length. Then $A \in \text{QIP}(m, c, s)$ if there exists an $m$-message quantum interactive proof system with the following properties:

1. **Completeness:** For all input strings $x \in A_{\text{yes}}$, there exists a prover that causes the verifier to accept with probability at least $c(|x|)$.

2. **Soundness:** For all input strings $x \in A_{\text{no}}$, every prover causes the verifier to accept with probability at most $s(|x|)$.

We define $\text{QIP}(m) = \text{QIP}(m, 2/3, 1/3)$, though Kitaev and Watrous proved in [KW00] that $\text{QIP}(m) = \text{QIP}(3, 1 - 2^{-p(n)}, 2^{-p(n)})$ for all $m \geq 3$ no larger than a polynomial in the input length. A recent breakthrough result in quantum computational complexity theory is that $\text{QIP} = \text{PSPACE}$ [JJUW10].

We also note that any promise problem in $\text{BQP}$ and $\text{QMA}$ can be decided by a quantum interactive proof system, as $\text{QIP}(0) = \text{BQP}$ and $\text{QIP}(1) = \text{QMA}$. This gives rise to a four-level quantum interactive proof hierarchy, ranging from the verifier alone to a verifier who exchanges no more than three messages with the prover. This hierarchy is shown in Figure 2 along with related classes. For more information about properties of $\text{QIP}(2)$ and $\text{QIP}(3)$ useful in the analysis of $\text{QSEP-STATE}_{1,1-\text{LOCC}}$ and $\text{QSEP-CHANNEL}_{1,1-\text{LOCC}}$, refer to Section 3.4 of [HMW13], as they are not directly applicable in our work here.

### 3.3.5 QSZK

Classical zero-knowledge proof systems were first considered by Goldwasser et al. in the same paper that introduced the classical interactive proof hierarchy [GMR89]. In their work they also introduced knowledge complexity as a measure of the amount of knowledge that the prover must transfer to the verifier in order to convince him of the truth of some statement. An interactive proof system for a language is said to be zero-knowledge if for every $x \in A_{\text{yes}}$, the prover can convince the verifier to accept without the verifier learning anything that he could not have computed himself. In statistical zero knowledge, this means that in a YES instance, the interaction with the prover has to be below some constant in trace distance (traditionally $1/10$) to a distribution corresponding to a computation that the verifier could have performed himself.

Quantum statistical zero-knowledge extends this definition to apply to a quantum interactive proof system instead [Wat02, Wat09b], with the requirement being that in a YES instance a computationally bounded quantum computer could simulate the verifier’s state at any point to within some constant trace distance.

**Definition 6 (QSZK)** A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\text{QSZK}(c, s)$ if there exists a statistical zero-knowledge quantum interactive proof system that satisfies the following properties:

1. **Completeness:** For all input strings $x \in A_{\text{yes}}$, the prover can convince the verifier to accept with probability at least $c(|x|)$.
2. Soundness: For all input strings \( x \in A_{\text{no}} \), the prover can convince the verifier to accept with probability at most \( s(|x|) \).

The traditional definition of \( \text{QSZK} \) is \( \text{QSZK}(2/3, 1/3) \), though \cite{Wat02} proved that \( \text{QSZK} = \text{QSZK}(1-2^{-p(n)}, 2^{-p(n)}) \) for any polynomial function \( p(n) \). Several facts are known about \( \text{QSZK} \): it is closed under complement, any \( \text{QSZK} \) proof system can be parallelized to two messages, and honest-verifier \( \text{QSZK} \) is equal to \( \text{QSZK} \) with a potentially cheating verifier \cite{Wat09}. The canonical \( \text{QSZK} \)-complete problem is \textsc{Quantum-State-Distinguishability}, commonly abbreviated \( \text{QSD} \), and defined as follows:

\begin{problem}[\textsc{Quantum-State-Distinguishability}] Fix a constant \( \varepsilon \in [0,1) \). Given is a mixed-state quantum circuit to generate the \( n \)-qubit states \( \rho_0 \) and \( \rho_1 \). Decide whether
\begin{enumerate}
  \item Yes: \( \|\rho_0 - \rho_1\|_1 \geq 2 - \varepsilon \).
  \item No: \( \|\rho_0 - \rho_1\|_1 \leq \varepsilon \).
\end{enumerate}
\end{problem}

3.3.6 \textbf{SQG}

After considering quantum interactive proofs with a single prover, it is natural to consider some variations on that theme. Short quantum games are one such variation in which two provers compete with each other. One prover—the yes-prover—attempts to convince the verifier to accept while the other prover—the no-prover—attempts to convince the verifier to reject. A short quantum game is a very restricted protocol of the following form:
Figure 3: Quantum circuit for a short quantum game. The yes-prover first sends a quantum message to the verifier, and the verifier performs some check (a unitary operation) on the transmitted quantum state. The verifier then sends a quantum message to the no-prover. The no-prover responds, and the verifier finally performs a unitary and a measurement to decide whether to accept or reject.

1. The verifier receives a single message from the yes-prover.

2. After processing the message from the yes-prover, the verifier prepares a message for the no-prover.

3. The no-prover replies to the verifier. After processing this response, the verifier decides whether to accept or reject.

A graphical depiction of a short quantum game is given in Figure 3. Short quantum games were first studied in [GW05], and the associated complexity class SQG was shown to collapse to PSPACE in [GW13].

**Definition 8 (SQG)** Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, and let $c, s : \mathbb{N} \to [0, 1]$ be polynomial-time computable functions. Then $A \in \text{SQG}(c, s)$ if there exists a verifier for a short quantum game satisfying the following properties:

1. **Completeness:** There exists a yes-prover such that, for all no-provers and for all input strings $x \in A_{\text{yes}}$, the yes-prover convinces the verifier to accept with probability at least $c(|x|)$.

2. **Soundness:** There exists a no-prover such that, for all yes-provers and for all input strings $x \in A_{\text{no}}$, the no-prover convinces the verifier to reject with probability at least $1 - s(|x|)$.

Every other complexity class discussed in this section is known to be robust with respect to the choice of completeness and soundness parameters $c, s$, meaning that any protocol for which $c$ is
larger than $s$ plus an inverse polynomial in the input length can be amplified into a new protocol with $c$ exponentially close to one and $s$ exponentially close to zero. However, the class SQG is not known to have such a property. Only a partial, “one-sided” amplification result is known, whereby $(c, s)$ can be amplified if $c$ is already exponentially close to one or $s$ is already exponentially close to zero [GW05]. It is an interesting open question whether the “logical-AND-of-majorities” error reduction technique [JUW09] for two-message quantum interactive proofs can be adapted to the competing provers setting.

4 QPROD-PURE-STATE is BQP-Complete

We begin with the simplest of our entanglement detection promise problems, that of determining if a quantum circuit generates a state close to a product state, in order to set the stage for the problems in the upcoming sections. Unlike the problems in the subsequent sections, the analysis of QPROD-PURE-STATE does not require the help of a prover, and as such, it is a straightforward application of the prior results of Harrow and Montanaro [HM10] combined with a reduction from a general BQP circuit.

Problem 9 (QPROD-PURE-STATE($\delta_c, \delta_s$)) Given is a description of a quantum circuit to generate the $n$-qubit pure state $|\psi\rangle_{A_1 \cdots A_l}$, along with a labeling of the output qubits for systems $A_1, \ldots, A_l$. Decide whether

1. Yes: There is a product state $|\phi_1\rangle_{A_1} \otimes \cdots \otimes |\phi_l\rangle_{A_l}$ that is $\delta_c$-close to $|\psi\rangle_{A_1 \cdots A_l}$ in trace distance:

$$\min_{|\phi_1\rangle, \ldots, |\phi_l\rangle} \left\| |\psi\rangle_{A_1 \cdots A_l} - |\phi_1\rangle_{A_1} \otimes \cdots \otimes |\phi_l\rangle_{A_l} \right\|_1 \leq \delta_c.$$

(11)

2. No: Every product state is at least $\delta_s$-far from $|\psi\rangle_{A_1 \cdots A_l}$ in trace distance:

$$\min_{|\phi_1\rangle, \ldots, |\phi_l\rangle} \left\| |\psi\rangle_{A_1 \cdots A_l} - |\phi_1\rangle_{A_1} \otimes \cdots \otimes |\phi_l\rangle_{A_l} \right\|_1 \geq \delta_s.$$

(12)

Theorem 10 QPROD-PURE-STATE($\delta_c, \delta_s$) is BQP-complete if there are polynomial-time computable functions $\delta_c, \delta_s : \mathbb{N} \rightarrow [0, 1]$ such that the difference $\frac{11}{2048} \delta_s^2 - \frac{1}{2} \delta_c^2$ is larger than an inverse polynomial in the circuit size.

Proof. We first show that QPROD-PURE-STATE($\delta_c, \delta_s$) $\in$ BQP. The BQP algorithm for deciding QPROD-PURE-STATE($\delta_c, \delta_s$) is to generate two copies of the state $|\psi\rangle_{A_1 \cdots A_l}$ by running the circuit twice, then to perform SWAP tests over each of the pairs of $l$ systems separately, and to accept if and only if all SWAP tests pass. This procedure is known as the product test [MCKB05 HM10].

The promise in (11) implies that

$$\max_{\phi_1, \ldots, \phi_l} |\langle \psi | \phi_1 \otimes \cdots \otimes \phi_l \rangle|^2 \geq 1 - \frac{\delta_c^2}{4},$$

by employing the Fuchs-van-de-Graaf equality in (5). The promise in (12) likewise implies that

$$\max_{\phi_1, \ldots, \phi_l} |\langle \psi | \phi_1 \otimes \cdots \otimes \phi_l \rangle|^2 \leq 1 - \frac{\delta_s^2}{4}.$$

14
Harrow and Montanaro have determined bounds on the success probability of the product test in Theorem 1 of [HM10]. The verifier accepts if every swap test passes, the probability of which is no smaller than $1 - \frac{\delta^2}{2}$ in a YES case, while in a NO case the probability of every swap test passing is no larger than $1 - \frac{11\delta^2}{2048}$. Thus, so long as

$$\frac{11}{2048}\delta^2 - \frac{1}{2}\delta^2_c$$

is larger than an inverse polynomial in the circuit size, repetition of this procedure no more than a polynomial number of times is sufficient to place the problem in \textbf{BQP}.

We now show that \textbf{QPROD-PURE-STATE} is \textbf{BQP}-hard. Let $U$ denote a quantum circuit for an arbitrary promise problem in \textbf{BQP} acting on $p(n)$ qubits with completeness and soundness error each less than $\varepsilon$, where the decision to accept or reject is based on a measurement of one of the output qubits (the decision qubit) in the computational basis.

We reduce this circuit to \textbf{QPROD-PURE-STATE} by appending three qubits in the state $|0\rangle_{A_1} |\Phi^+\rangle_{A_2A_3}$ to the output of the \textbf{BQP} circuit $U$. We perform a bit flip on the decision qubit and a controlled-SWAP from the decision qubit to the qubits in systems $A_1$ and $A_2$. The resulting state is as follows:

$$|\psi\rangle_{DGA_1A_2A_3} \equiv (|1\rangle(1 | D \otimes I_G)|\phi\rangle_{DG}) |0\rangle_{A_1} |\Phi^+\rangle_{A_2A_3} + (|0\rangle(0 | D \otimes I_G)|\phi\rangle_{DG}) |0\rangle_{A_2} |\Phi^+\rangle_{A_1A_3},$$

where $|\phi\rangle_{DG}$ denotes the state $U |0\rangle^{\otimes p(n)}$. This reduction is shown in Figure 4.

We could then feed the result of this computation into an instance of \textbf{QPROD-PURE-STATE} and use an algorithm that decides \textbf{QPROD-PURE-STATE} to determine whether the state is product.
(or close to product) with respect to the bipartite cut $DGA_1 : A_2 A_3$. Given an arbitrary problem in BQP with completeness and soundness error $\varepsilon$, then in a YES instance the following acceptance probability is high:

$$\|\langle 1 \rangle_D \otimes I_G | \phi \rangle_{DG} \|^2_2 \geq 1 - \varepsilon.$$ 

Thus, after performing the additional steps mentioned above, the resulting state $|\psi\rangle_{DGA_1 A_2 A_3}$ has a high fidelity with

$$|\phi\rangle_{DG} \otimes |0\rangle_{A_1} \otimes |\Phi^+\rangle_{A_2 A_3}$$

because

$$\left| \langle \psi |_{DGA_1 A_2 A_3} \left( |\phi\rangle_{DG} \otimes |0\rangle_{A_1} \otimes |\Phi^+\rangle_{A_2 A_3} \right) \right|^2 \geq |\langle \phi |_{DG} \langle 1 \rangle_D \otimes I_G | \phi \rangle_{DG} |^2 = \|\langle 1 \rangle_D \otimes I_G | \phi \rangle_{DG} \|^2_2 \geq 1 - \varepsilon.$$ 

By the Fuchs-van-de-Graaf inequalities, it then follows that

$$\|\| \langle \psi |_{DGA_1 A_2 A_3} - |\phi\rangle_{DG} \otimes |0\rangle_{A_1} \otimes |\Phi^+\rangle_{A_2 A_3} \| \leq 2\sqrt{2}\varepsilon,$$

so that the state is approximately product with respect to the bipartite cut $DGA_1 : A_2 A_3$, and thus

$$\min_{|\zeta\rangle, |\theta\rangle} \|\| \langle \psi |_{DGA_1 A_2 A_3} - |\zeta\rangle_{DGA_1} \otimes |\theta\rangle_{A_2 A_3} \| \leq 2\sqrt{2}\varepsilon. \quad (13)$$

So a YES instance of any promise problem in BQP reduces to a YES instance of QPROD-PURE-STATE.

On the other hand, in the case of a NO instance, the following rejection probability is high:

$$\|\langle 0 \rangle_D \otimes I_G | \phi \rangle_{DG} \|^2_2 \geq 1 - \varepsilon.$$ 

Thus, after performing the additional steps mentioned above, the resulting state $|\psi\rangle_{DGA_1 A_2 A_3}$ has a high overlap with

$$|\phi\rangle_{DG} \otimes |0\rangle_{A_2} \otimes |\Phi^+\rangle_{A_1 A_3},$$

because

$$\left| \langle \psi |_{DGA_1 A_2 A_3} \left( |\phi\rangle_{DG} \otimes |0\rangle_{A_2} \otimes |\Phi^+\rangle_{A_1 A_3} \right) \right|^2 \geq |\langle \phi |_{DG} \langle 0 \rangle_D \otimes I_G | \phi \rangle_{DG} |^2 = \|\langle 0 \rangle_D \otimes I_G | \phi \rangle_{DG} \|^2_2 \geq 1 - \varepsilon.$$ 

Now, we consider the maximum separable fidelity $[Wat04, HMW13, CAH13]$ of $|\phi\rangle_{DG} \otimes |0\rangle_{A_2} \otimes |\Phi^+\rangle_{A_1 A_3}$ with respect to the cut $DGA_1 : A_2 A_3$

$$\max_{\sigma_{DGA_1 : A_2 A_3} \in S} F \left( |\phi\rangle_{DG} \otimes |0\rangle_{A_2} \otimes |\Phi^+\rangle_{A_1 A_3}, \sigma_{DGA_1 : A_2 A_3} \right). \quad (14)$$

Since the first state is pure, the fidelity takes the special form

$$\langle \phi \rangle_{DG} (0)_{A_2} \langle \Phi^+ \rangle_{A_1 A_3} \sigma_{DGA_1 : A_2 A_3} |\phi\rangle_{DG} (0)_{A_2} |\Phi^+\rangle_{A_1 A_3}.$$
and it is clear that a pure product state optimizes (14). Furthermore, it is clear that we can take the state $\sigma$ on the systems $DG$ and $A_2$ to be $|\phi\rangle_{DG}|0\rangle_{A_2}$ since this state is product with respect to the cut $DGA_1 : A_2A_3$. We find that (14) is equal to
\[
\max_{|\zeta\rangle,|\theta\rangle} \left| \langle \Phi^+ | A_1A_3 | \zeta \rangle A_1 | \theta \rangle A_3 \right|^2 = \frac{1}{2},
\]
where the equality follows from \[Wat04\]. Exploiting the Fuchs-van-de-Graaf inequalities once again, we find that
\[
\left\| \langle \psi \rangle \langle \psi \rangle_{DG A_1 A_2 A_3} - |\phi\rangle \langle \phi \rangle_{DG} \otimes |0\rangle \langle 0 |_{A_2} \otimes \Phi^+_{A_1 A_3} \right\|_1 \leq 2\sqrt{2\varepsilon},
\]

\[
\min_{|\zeta\rangle,|\theta\rangle} \left\| |\phi\rangle \langle \phi | \otimes |0\rangle \langle 0 |_{A_2} \otimes \Phi^+_{A_1 A_3} - |\zeta\rangle \langle \zeta | \otimes |\theta\rangle \langle \theta |_{A_2 A_3} \right\|_1 \geq 2 \left( 1 - \frac{1}{\sqrt{2}} \right) \geq \frac{1}{2}.
\]

Using the triangle inequality, we end up with
\[
\min_{|\zeta\rangle,|\theta\rangle} \left\| |\psi\rangle \langle \psi | \otimes |0\rangle \langle 0 |_{DG A_1 A_2 A_3} - |\zeta\rangle \langle \zeta | \otimes |\theta\rangle \langle \theta |_{A_2 A_3} \right\|_1 \geq \frac{1}{2} - 2\sqrt{2\varepsilon},
\]
so that a NO instance of any promise problem in BQP reduces to a NO instance of QPROD-PURE-STATE. Since the gap between the lower bound in (15) and the upper bound in (13) is equal to a positive constant $1/2 - 4\sqrt{2}\varepsilon$ for small enough $\varepsilon$, it follows that QPROD-PURE-STATE is BQP-hard.

5 QSEP-ISOMETRY$_{1,1}$-LOCC is QMA-Complete

In this section, we give a proof of the QMA-completeness of QSEP-ISOMETRY$_{1,1}$-LOCC, the problem of determining if an isometry can generate a state close to some separable state in the trace distance or if all inputs to the isometry lead to a state far from all separable states in the one-way LOCC distance. There are many other problems known to be QMA-complete, including the problem of testing whether a quantum channel (specified by a mixed-state quantum circuit) is not close to an isometry \[Ros11\], estimating the ground state of a $k$-local Hamiltonian \[KKR06, KŠV02\] and many more (see \[Boo12\] for an overview). Nonetheless, it is of interest to note that this problem is QMA-complete when the soundness condition is defined in terms of the one-way LOCC distance, in comparison to the result in the subsequent section that QSEP-ISOMETRY, which is defined in terms of the trace distance when there are no subscripts, is QMA(2)-complete.

**Problem 11** (QSEP-ISOMETRY$_{1,1}$-LOCC($\delta_c, \delta_s$)) *Given is a description of a quantum circuit to implement a unitary $U$ acting on an $n$-qubit input and $m$ ancilla qubits, as well as a labeling of the systems $A_1, \ldots, A_l$. Decide whether*

1. **Yes:** There is an input $\rho_S$ such that the output of $U$ is $\delta_c$-close in trace distance to a separable state:
\[
\min_{\rho,\sigma_A \in S} \left\| U(\rho_S \otimes |0\rangle \langle 0|^\otimes m )U^\dagger - \sigma_{A_1 \ldots A_l} \right\|_1 \leq \delta_c.
\]
2. No: For all inputs $\rho_S$, the output of $U$ is at least $\delta_s$-far in 1-LOCC distance from a separable state:

$$\min_{\rho, \sigma_{A_1 \cdots A_l} \in \mathcal{E}_k} \left\| U(\rho \otimes \ket{0}^{\otimes m})U^\dagger - \sigma_{A_1 \cdots A_l} \right\|_{1\text{-LOCC}} \geq \delta_s.$$  \hspace{1cm} (17)

**Theorem 12** QSEP-ISOMETRY$_{1,1\text{-LOCC}}(\delta_c, \delta_s)$ is QMA-complete if there are polynomial-time computable functions $\delta_c, \delta_s : \mathbb{N} \to [0, 1]$ such that the difference $\delta_c^2/8 - 4\sqrt{\delta_c}$ is larger than an inverse polynomial in the circuit size.

**Proof.** We first show that QSEP-ISOMETRY$_{1,1\text{-LOCC}}(\delta_c, \delta_s) \in \text{QMA}$ by adapting the $k$-extension testing method from [HMW13]. First, note that by Lemma 26 in Appendix A.2, the condition in (16) implies the existence of pure states $|\psi\rangle, |\phi_1\rangle, \ldots, |\phi_l\rangle$ such that

$$\left\| U(|\psi\rangle \langle \psi|_S \otimes |0\rangle^{\otimes m})U^\dagger - |\phi_1\rangle \langle \phi_1|_{A_1} \otimes \cdots \otimes |\phi_l\rangle \langle \phi_l|_{A_l} \right\|_1 \leq 4\sqrt{\delta_c}.$$  \hspace{1cm} (18)

In a YES instance, the prover can provide the state $|\psi\rangle$ and $k$ copies of the states $|\phi_1\rangle, \ldots, |\phi_l\rangle$ to the verifier. The verifier then runs $U$ on $|\psi\rangle_S \otimes |0\rangle^{\otimes m}$ to generate a state close to $|\phi_1\rangle_{A_1} \otimes \cdots \otimes |\phi_l\rangle_{A_l}$ and performs a permutation test over all copies on each of the systems (see Section 8 of [HMW13] for details of the permutation test). The promise in (16) implies that the permutation test will succeed with probability at least $1 - 4\sqrt{\delta_c}$ for any $k$. This follows from applying (1) to (18).

In a NO instance, we can employ the promise in (17) and Lemma 1 by requiring $k$ to be larger than

$$\left\lfloor l + \frac{4l^2(n + m)}{(\delta_s - \delta'_s)^2} \right\rfloor,$$

in order to guarantee that

$$\min_{\rho, \sigma_{A_1 \cdots A_l} \in \mathcal{E}_k} \left\| U(\rho \otimes |0\rangle^{\otimes m})U^\dagger - \sigma_{A_1 \cdots A_l} \right\|_{1\text{-LOCC}} \geq \delta'_s,$$

for $\delta'_s$ strictly less than $\delta_s$, which can be enforced by setting $\delta'_s = \delta_s / \sqrt{2}$. By an analysis similar to that in Section 8 of [HMW13], we find the following bound on the probability that the permutation test succeeds:

$$\max_{\rho, \sigma_{A_1 \cdots A_l} \in \mathcal{E}_k} F(U(\rho \otimes |0\rangle^{\otimes m})U^\dagger, \sigma_{A_1 \cdots A_l}) \leq 1 - \delta'_s^2/8.$$

Note that $l$ cannot be larger than the total number of qubits acted upon, and thus the promise that $\delta'_s^2/8 - 4\sqrt{\delta_c}$ is larger than an inverse polynomial is sufficient to place the problem in QMA.

The QMA-hardness of QSEP-ISOMETRY$_{1,1\text{-LOCC}}$ follows similarly to how we proved BQP-hardness of QPROD-PURE-STATE, by swapping a Bell state across the output systems controlled on the decision qubit being equal to $|0\rangle$. This reduction is shown in Figure 5. This reduction creates a unitary for which the analysis in a YES instance proceeds identically to the analysis in Section 4 so that a YES instance of a general QMA problem becomes a YES instance of QSEP-ISOMETRY$_{1,1\text{-LOCC}}$ with $\delta_c = 2\sqrt{2}\varepsilon$.

In a NO instance, we wish to show that the one-way LOCC distance from the output of the circuit in Figure 5 to the nearest separable state is larger than an appropriate constant. To show this, we proceed by using the $A_1$ and $A_3$ systems in the CHSH game (a reformulation of a Bell experiment as a nonlocal game [CHTW04]), so that we can distinguish the output of the circuit.
from all separable states by means of a one-way LOCC protocol. In such a protocol, we imagine that Alice has system $A_1$ and flips a coin $x$ to choose one of two binary-outcome measurements to perform on her qubit. She sends both $x$ and the measurement outcome $a$ to Bob who we imagine has system $A_3$. Bob then flips a coin $y$ and performs one of two binary outcome measurements on his qubit, naming the measurement result $b$. Bob declares the state to be a Bell state in the case that $x \land y = a \oplus b$ and otherwise declares that it is not. It is well known that the probability of winning such a game with a Bell state is equal to $\cos^2(\pi/8) \approx 0.85$, while the maximum probability of winning such a game with any separable state is equal to 0.75 [CHTW04]. From this, we can easily lower bound the one-way LOCC distance of the final state from the reduction:

$$\min \rho, \sigma_{DGA_1:A_2A_3} \in S \| V(\rho_S \otimes |0\rangle\langle 0|^{\otimes m}) V^\dagger - \sigma_{DGA_1:A_2A_3} \|_{1-LOCC}$$

$$\geq \| \Phi^+_{A_1A_3} - \sigma_{A_1:A_3} \|_{1-LOCC}$$

$$- \| \Phi^+_{A_1A_3} - \text{Tr}_{DGA_2} \{ V(\rho_S \otimes |0\rangle\langle 0|^{\otimes m}) V^\dagger \} \|_{1-LOCC}$$

$$\geq 0.2 - 2\sqrt{\varepsilon},$$

where $V$ denotes the transformation realized by $U$ and the controlled-SWAP and $1 - \varepsilon$ is a lower bound on the fidelity between the state of the decision qubit and $|0\rangle$ as in the BQP reduction. The second inequality follows from the fact that the fidelity of $V(\rho_S \otimes |0\rangle\langle 0|^{\otimes m}) V^\dagger$ with $\Phi^+$ over the $A_1 : A_3$ system is equal to the fidelity of the decision qubit with $|0\rangle$ (due to the controlled swap). After the reduction, then, this becomes an instance of QSEP-ISOMETRY$_{1,1-LOCC}$ with $\delta_s = 0.2 - 2\sqrt{\varepsilon}$.

Thus, as long as $\varepsilon$ is small enough (so that $0.2 - (2 + 2\sqrt{2})\sqrt{\varepsilon} > 0$), there is an appropriate gap between the completeness and soundness errors, and QSEP-ISOMETRY$_{1,1-LOCC}$ is thus QMA-hard.
This concludes the proof that \( \text{QSEP-ISOMETRY}_{1,1,\text{-LOCC}} \) is \( \text{QMA} \)-complete. ■

6 QPROD-ISOMETRY and QSEP-ISOMETRY are \( \text{QMA}(2) \)-Complete

In this section, we show that QPROD-ISOMETRY, the problem of determining if an isometry can produce a state close to a product state (in the trace distance), is \( \text{QMA}(2) \)-complete. We also demonstrate that it is equivalent to the problem QSEP-ISOMETRY, the trace distance version of QSEP-ISOMETRY\(_{1,1,\text{-LOCC}}\) from the previous section. It is clear that being able to detect productness in the trace distance is of considerable use; for one, it allows a verifier to force two unentangled provers to simulate \( k \) unentangled provers as shown in the proof that \( \text{QMA}(2) = \text{QMA}(k) \) [HMI10].

It seems intuitive then that these problems in the trace distance can neatly capture the power of “unentanglement,” an intuition that we make precise in what follows.

Problem 13 (QPROD-ISOMETRY\((\delta_c, \delta_s)\)) Given is a description of a quantum circuit to implement a unitary \( U \) acting on an \( n \)-qubit input and \( m \) ancilla qubits, as well as a labeling of the systems \( A_1, \ldots, A_l \). Decide whether

1. Yes: There is an input \( \rho \) such that the output of \( U \) is \( \delta_c \)-close in trace distance to a product state:

\[
\min_{\rho, \sigma_{A_1 \cdots A_l} \in \mathcal{P}} \left\| U(\rho_S \otimes |0\rangle \langle 0|^m)U^\dagger - \sigma_{A_1 \cdots A_l} \right\|_1 \leq \delta_c.
\]  

(19)

2. No: For all inputs \( \rho \), the output of \( U \) is at least \( \delta_s \)-far in trace distance from a product state:

\[
\min_{\rho, \sigma_{A_1 \cdots A_l} \in \mathcal{P}} \left\| U(\rho_S \otimes |0\rangle \langle 0|^m)U^\dagger - \sigma_{A_1 \cdots A_l} \right\|_1 \geq \delta_s.
\]  

(20)

Theorem 14 QPROD-ISOMETRY\((\delta_c, \delta_s)\) is \( \text{QMA}(2) \)-complete if there are polynomial-time computable functions \( \delta_c, \delta_s : \mathbb{N} \to [0, 1] \) such that the difference \( \frac{1162}{3096} - 8\delta_c \) is larger than an inverse polynomial in the circuit size.

Proof. We first show that QPROD-ISOMETRY is in \( \text{QMA}(l+1) \), from which it follows by [HMI10] that it is in \( \text{QMA}(2) \). Our proof system has \( l+1 \) provers send the minimizing input and each part of the minimizing product state, followed by the verifier performing the unitary \( U \) on the input and then the product test on the provided product state.

Let \( \omega_{A_1 \cdots A_l} \) denote the state that results after the verifier performs the unitary \( U \) on the input \( \rho_S \) received from the first prover, and let \( \sigma_{A_1 \cdots A_l} \) denote the product state received from the other \( l \) provers. Lemma 2 of [HMI10] establishes the following formula for the success probability of the product test:

\[
P_{\text{test}}(\omega_{A_1 \cdots A_l}, \sigma_{A_1 \cdots A_l}) = \frac{1}{2^l} \sum_{S \subseteq \{A_1, \ldots, A_l\}} \text{Tr}\{\omega_S \sigma_S\}.
\]

In particular, it is clear by a convexity argument that it is optimal for the last \( l \) provers to send pure quantum states to the verifier. That is, for every set of mixed states that they could send,
there exists a set of pure states that gives the same or higher probability of passing the product test. So we can assume without loss of generality that the last $l$ provers send pure states.

We now analyze the YES instance. By Lemma 26, the condition in (19) implies that there exist pure states $\psi, \phi_1, \ldots, \phi_l$ such that

$$
\left\| U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|^m)U^\dagger - |\phi_1\rangle\langle\phi_1|_{A_1} \otimes \cdots \otimes |\phi_l\rangle\langle\phi_l|_{A_l} \right\|_1 \leq 4\sqrt{\delta_c}.
$$

Thus, in a YES instance, the $l+1$ provers can provide the states $\psi, \phi_1, \ldots, \phi_l$, respectively, so that running the product test between $U(|\psi\rangle\langle0|^m)U^\dagger$ and $\phi_1 \otimes \cdots \otimes \phi_l$ will succeed with probability no smaller than $1 - 8\delta_c$.

We now analyze the NO instance. The promise in (20) then gives the following upper bound on $\delta_s$:

$$
\delta_s \leq \min_{\rho, \sigma, A_1 \cdots A_l \in P} \left\| U(\rho \otimes |0\rangle\langle0|^m)U^\dagger - \sigma_{A_1 \cdots A_l} \right\|_1
$$

$$
\leq 2\sqrt{1 - \max_{\rho, \sigma, A_1 \cdots A_l \in P} F(U(\rho \otimes |0\rangle\langle0|^m)U^\dagger, \sigma_{A_1 \cdots A_l})}
$$

$$
\leq 2\sqrt{1 - \max_{\rho, \sigma, A_1 \cdots A_l \in P} \left( \text{Tr}(U(\rho \otimes |0\rangle\langle0|^m)U^\dagger \sigma_{A_1 \cdots A_l}) \right)^2}
$$

$$
= 2\sqrt{1 - \max_{\psi, \phi_1, \ldots, \phi_l} |\langle(\psi_S|\otimes (0)^m)U^\dagger |\phi_1\rangle \otimes \cdots \otimes |\phi_l\rangle|^2}
$$

The second inequality is an application of the Fuchs-van-de-Graaf inequalities. The third inequality follows from $F(\rho, \sigma) = (\text{Tr}(|\sqrt{\rho}\sqrt{\sigma}|))^2 \geq (\text{Tr}(|\sqrt{\rho}|^2))^2 \geq (\text{Tr}(\rho))^2$. The final inequality follows from a convexity argument (for every set of mixed states, there is a set of pure states that can achieve the same or higher value, so that it suffices to maximize over pure states). We can rewrite the above bound as follows:

$$
\max_{\psi, \phi_1, \ldots, \phi_l} |\langle(\psi_S|\otimes (0)^m)U^\dagger |\phi_1\rangle \otimes \cdots \otimes |\phi_l\rangle|^2 \leq \sqrt{1 - \delta_s^2/4} \leq 1 - \delta_s^2/8.
$$

By Theorem 1 of [HIM10], we can then conclude that the probability of the product test succeeding is no greater than $1 - \frac{11\delta_s^2}{24}$. Thus, the promise in Theorem 14 is sufficient for the verifier to decide this instance. We have now placed QPROD-ISOMETRY in QMA($l+1$) and further in QMA(2) by applying the exponential amplification result of [HIM10].

To show that QPROD-ISOMETRY is QMA(2)-hard, consider an arbitrary QMA(2) circuit acting on $p(n)$ qubits with completeness and soundness error at most $\varepsilon$. On an input $x$, we describe the verifier’s corresponding unitary as $V_x : ABW \rightarrow DG$, which takes two product inputs from the provers on the $A$ and $B$ systems respectively along with ancilla qubits in the $|0\rangle$ state on the $W$ system, and outputs a decision qubit (labeled as $D$) along with a reference system $G$. Note that any QMA(2) verifier can be expressed in this way. The circuit $V_x$ is depicted in Figure 3(a).

We reduce any QMA(2) proof system to QPROD-ISOMETRY by constructing a circuit $U : DGCC' \rightarrow A_1A_2$ shown in Figure 5(b) as follows:

1. Prepare a Bell state across the ancilla registers $C, C'$.
2. Prepare the $D$ register in the state $|1\rangle$ and perform $V_x^\dagger$ on the registers $DG$ to obtain the registers $ABW$. 

21
Figure 6: (a) The unitary circuit \( V_x \) for an arbitrary \( \text{QMA}(2) \) verifier on input \( x \). Such a verifier has two quantum witness registers, \( A \) and \( B \), inputs to which are provided by the two unentangled provers. The verifier initializes an ancilla register \( W \) to the all-zero state \( |0\rangle \) and performs the unitary \( V_x \). This procedure produces a single-qubit decision register \( D \), the measurement of which indicates acceptance or rejection, and a register \( G \) which is ignored. (b) The circuit \( U \) produced by our reduction. The verifier’s circuit \( V_x \) is inverted and the decision register is initialized to \( |1\rangle \). After \( V_x^\dagger \) is applied, the register \( W \) controls whether the Bell states are swapped in to cause the output to be entangled.

3. Perform the following “controlled swap” gate:

\[
(|0\rangle\langle 0|^{\otimes m})_W \otimes I_{AC'} + (I^{\otimes m} - |0\rangle\langle 0|^{\otimes m})_W \otimes \text{SWAP}_{AC'},
\]

4. Label the \( A \) register as \( A_1 \) and the \( CC'BW \) registers as \( A_2 \).

We begin by showing that such a circuit can produce a state close to product if there is an accepting input to \( V_x \), and then that the circuit can only produce states that are far from separable if no such accepting input exists. (Note that the state is far from being product if it is far from being separable because \( P \in \mathcal{S} \).)

In the case of a YES instance of the \( \text{QMA}(2) \) problem, by a convexity argument, we know that there are pure states \( |\phi\rangle_A \) and \( |\psi\rangle_B \) such that

\[
\langle 1|_D \text{Tr}_G \{V_x (|\phi\rangle_A \otimes |\psi\rangle_B \otimes (|0\rangle^{\otimes m})_W) V_x^\dagger \} |1\rangle_D \geq 1 - \varepsilon.
\]

By Uhlmann’s theorem, this means that there also exists a pure state \( |\zeta\rangle_G \) such that

\[
|\langle 1|_D \langle\zeta|_G V_x (|\phi\rangle_A \otimes |\psi\rangle_B \otimes (|0\rangle^{\otimes m})_W)|^2 \geq 1 - \varepsilon.
\]

Thus, there exists an input \( |\zeta\rangle_G \) to the circuit \( U \) such that the output will have a large overlap with the state \( |\phi\rangle_A \otimes |\psi\rangle_B \otimes |\Phi^+\rangle_{CC'} \otimes (|0\rangle^{\otimes m})_W \) (1 − \( \varepsilon \) of the weight of the state after \( V_x^\dagger \) acts is on \( (|0\rangle^{\otimes m})_W \), so that the controlled-SWAP acts almost as the identity). The state \( |\phi\rangle_A \otimes |\psi\rangle_B \otimes |\Phi^+\rangle_{CC'} \otimes (|0\rangle^{\otimes m})_W \) is product across the cut \( A : BCC'W \), so that we map a YES instance of a general \( \text{QMA}(2) \) proof system to a YES instance of \( \text{QPROD-ISOMETRY} \).
Now, let $x$ be a NO instance. Beginning with the pure case, we have a promise that there is no product input to $V_x$ such that the probability of measuring $|1\rangle$ on the decision qubit is larger than $\varepsilon$:

$$\max_{|\phi\rangle_A, |\psi\rangle_B} (1)_D \text{Tr}_G \{ V_x (|\phi\rangle_A \otimes |\psi\rangle_B \otimes (|0\rangle \otimes m)_W) V_x^\dagger \} |1\rangle_D \leq \varepsilon. \quad (27)$$

By Uhlmann’s theorem, the above is equivalent to

$$\max_{|\phi\rangle_A, |\psi\rangle_B, |\zeta\rangle_G} |\langle 1|_D \langle \zeta|_G V_x (|\phi\rangle_A \otimes |\psi\rangle_B \otimes (|0\rangle \otimes m)W) |1\rangle_D \zeta\rangle_G|^2 \leq \varepsilon. \quad (28)$$

To show that the output of the circuit $U$ is far from a product state for any input on the system $G$, we will bound the following quantity:

$$\max_{|\zeta\rangle, |\sigma\rangle_{ACC'BW} \in \mathcal{P}} \left| \langle \sigma|_{ACC'BW} U |\Phi^+\rangle_{CC'} |1\rangle_D \zeta\rangle_G \right|,$n

where $|\sigma\rangle$ is product across the $A:CC'BW$ cut. To do so, note that the state $|\sigma\rangle$ can be written as the following superposition:

$$|\sigma\rangle_{ACC'BW} = \alpha_0 |0\rangle_W |\sigma_0\rangle_{ACC'B} + \alpha_1 |1\rangle_W |\sigma_1\rangle_{ACC'B}, \quad (30)$$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$. (In the above, we are now modeling the system $W$ as a qubit in which $|0\rangle$ represents the projection onto the all-zeros state of $m$ qubits and $|1\rangle$ represents the projection onto the complementary space. It suffices for us to do since we are only interested in these two subspaces.) Also, note that both $|\sigma_0\rangle_{ACC'B}$ and $|\sigma_1\rangle_{ACC'B}$ are product across the bipartite cut $A:CC'B$ since $|\sigma\rangle_{ACC'BW}$ is. Substituting (30) into (29), we find that

$$\max_{|\zeta\rangle, |\sigma\rangle_{ACC'BW} \in \mathcal{P}} \left| \langle \sigma|_{ACC'BW} U |\Phi^+\rangle_{CC'} |1\rangle_D \zeta\rangle_G \right| = \max_{|\zeta\rangle, |\sigma\rangle_{ACC'BW} \in \mathcal{P}} \left| \alpha_0 (0)_W \langle \sigma_0|_{ACC'B} |\Phi^+\rangle_{CC'} V_x^\dagger |1\rangle_D \zeta\rangle_G \right| + \alpha_1 (1)_W \langle \sigma_1|_{ACC'B} \text{SWAP}_{AC'} |\Phi^+\rangle_{CC'} V_x^\dagger |1\rangle_D \zeta\rangle_G \right|$$

$$\leq \max_{|\zeta\rangle, |\sigma\rangle_{ACC'BW} \in \mathcal{P}} \left| (0)_W \langle \sigma_0|_{ACC'B} |\Phi^+\rangle_{CC'} V_x^\dagger |1\rangle_D \zeta\rangle_G \right| + \max_{|\zeta\rangle, |\sigma\rangle_{ACC'BW} \in \mathcal{P}} \left| (1)_W \langle \sigma_1|_{ACC'B} \text{SWAP}_{AC'} |\Phi^+\rangle_{CC'} V_x^\dagger |1\rangle_D \zeta\rangle_G \right|$$

$$\leq \max_{|\phi\rangle_A, |\psi\rangle_B, |\zeta\rangle_G} \left| (0)_W \otimes \langle \phi|_A \otimes \langle \psi|_B V_x^\dagger |1\rangle_D \zeta\rangle_G \right| + \max_{\sigma_{AC} \in \mathcal{S}} \sqrt{F(\sigma_{AC}, \Phi_{AC})} \leq \sqrt{\varepsilon} + \frac{1}{\sqrt{2}}.$$

The first inequality follows from the triangle inequality and the fact that $|\alpha_i| \leq 1$ since $|\alpha_i|^2 \leq 1$. The second inequality follows from the monotonicity of fidelity under the tracing out of registers ($C$ and $C'$ for the first term and $C'$, $B$, and $W$ for the second term). Restricting the optimization in the first term to be over pure product states follows by another simple convexity argument. Performing the optimization in the second term over all separable states can achieve only the same or a higher value for the fidelity since $P \in \mathcal{S}$. The final inequality follows from (28) and from the
fact that the maximum fidelity of a separable state with $|\Phi^+\rangle$ is $\frac{1}{2}$ [Wat04]. The analysis above easily generalizes to mixed states by observing that the maximization in (27) can be performed over mixed states and the rest of the analysis can proceed with the purification.

Using the Fuchs-van-de-Graaf inequality in (5), we can bound the trace distance as

$$\min_{\omega,\sigma: A \in \mathcal{P}} \|U(\omega \otimes |0\rangle\langle 0|^m)U^\dagger - \sigma\|_1 \geq \frac{\sqrt{2} - 1}{\sqrt{2}} - \sqrt{\varepsilon},$$

and so for a sufficiently small $\varepsilon$ there is an appropriate gap between the completeness and soundness errors. Thus, we have shown that under the stated promise $\text{QPROD-ISOMETRY}$ is both in $\text{QMA}(2)$ as well as $\text{QMA}(2)$-hard, and thus $\text{QMA}(2)$-complete.

**Corollary 15** $\text{QSEP-ISOMETRY}(\delta_c, \delta_s)$ is $\text{QMA}(2)$-complete if there are polynomial-time computable functions $\delta_c, \delta_s : \mathbb{N} \to [0, 1]$ such that the difference $\frac{11\delta_s^2}{2048} - 8\delta_c$ is larger than an inverse polynomial in the circuit size.

**Proof.** The main reason that this result follows easily is that allowing classical communication between the provers does not change $\text{QMA}(2)$. $\text{QSEP-ISOMETRY}$ is defined identically to $\text{QPROD-ISOMETRY}$ except that the minimizations in conditions (19) and (20) are over the set of separable states rather than the set of product states. To see that this problem is also in $\text{QMA}(2)$, note that the analysis for the inclusion of $\text{QPROD-ISOMETRY}$ in a YES instance applies to $\text{QSEP-ISOMETRY}$ as well, since Lemma 26 holds for separable states. The analysis of the NO instance proceeds identically.

Indeed, $\text{QSEP-ISOMETRY}$ is $\text{QMA}(2)$-hard by means of a very similar reduction as we used for $\text{QPROD-ISOMETRY}$. We proved that in a YES instance there is an input so that the output state close to product (and thus close to separable), while in a NO instance, a very similar analysis demonstrates that all inputs will lead to an output state that is far from separable.

### 7 QPROD-STATE is QSizK-Complete

In this section, we examine $\text{QPROD-STATE}$, which extends $\text{QPROD-PURE-STATE}$ to allow for quantum circuits that output mixed states (that is, the circuit outputs a reference system and another one but traces over the reference system). This addition of a reference system thwarts our ability to use the product test since (as noted in Section 4), the product test fails very quickly on mixed state inputs. In contrast to the $\text{BQP}$-complete pure-state version and the $\text{QMA}(2)$-complete isometry version, we show that this problem is $\text{QSizK}$-complete. This new result also leads to the rather surprising conclusion that $\text{QSEP-STATE}_{1,1,\text{LOCC}}$—even though it is stated with respect to the $1$-LOCC distance—is at least as hard as $\text{QPROD-STATE}$ despite the fact that $\text{QPROD-ISOMETRY}$ is harder than $\text{QSEP-ISOMETRY}_{1,1,\text{LOCC}}$ (if there is a strict separation between QMA and $\text{QMA}(2)$).

**Problem 16** ($\text{QPROD-STATE}(\delta_c, \delta_s)$) Given is a quantum circuit $U$ to generate the state $|\psi\rangle_{RC}$, along with a labelling of the qubits in the reference system $R$ and the output qubits for each system $A_1, A_2, \ldots, A_l \in C$. We define the $n$-qubit state $\rho_C = \text{Tr}_R(|\psi\rangle\langle \psi|_{RC})$. Decide whether

1. Yes: There exists a product state such that $\rho_C$ is $\delta_c$-close in trace distance to it:

$$\min_{\sigma_C \in \mathcal{P}} \|\rho_C - \sigma_C\|_1 \leq \delta_c. \quad (31)$$
2. No: Every product state is at least \( \delta_s \)-far in trace distance to \( \rho_C \):

\[
\min_{\sigma_C \in \mathcal{P}} \| \rho_C - \sigma_C \|_1 \geq \delta_s.
\] (32)

**Theorem 17** \( \text{QPROD-STATE}(\delta_c, \delta_s) \) is \( \text{QSZK} \)-complete if there are polynomial-time computable functions \( \delta_c, \delta_s : \mathbb{N} \rightarrow [0, 1] \) such that the difference \( \delta_s^2 / 4 - \delta_c \) is greater than an inverse polynomial in the circuit size.

**Proof.** We begin by giving a quantum statistical zero-knowledge proof system to decide \( \text{QPROD-STATE} \). Recall that a product state is of the form \( \rho_C = \rho_{A_1}^{I_1} \otimes \cdots \otimes \rho_{A_l}^{I_l} \). In the case that a state on \( C \) is exactly product, by Uhlmann’s theorem there exists an isometry that the prover can perform on the purifying system \( R \) to separate the purifications of each of the subsystems. Indeed, there exists some unitary \( P_{RR' \rightarrow R_1 \ldots R_l} \) acting on \( R \) and the prover’s system \( R' \) such that

\[
(P_{RR' \rightarrow R_1 \ldots R_l} \otimes I_C) |\psi\rangle_{RC} |0\rangle_R = |\psi\rangle_{R_1 A_1} \otimes |\psi\rangle_{R_2 A_2} \otimes \cdots \otimes |\psi\rangle_{R_l A_l},
\]

where \( R_1 \) purifies \( A_1 \) and so on. Since these purifications are arbitrary, we can take them such that \( R_1 \cong RA_2 A_3 \ldots A_l, R_2 \cong RA_1 A_3 \ldots A_l \) and so on.

For the proof system, the verifier need only send the reference system \( R \) to the prover, and if the state is close to product, the purifier should be able to provide the purification systems \( R_1, \ldots, R_l \) as above. The verifier then performs \( U^{\dagger} \) on each system pair \( R_1 A_1, \ldots, R_l A_l \) and measures the output, accepting if every measurement outcome is \( |0\rangle \). This proof system is depicted in Figure 7.

Note also that it is statistical zero-knowledge because, in the case of a YES instance, the verifier could have simply performed \( U \) exactly \( l \) times to create \( l \) copies of the state \( |\psi\rangle_{RC} \).

For the following analysis, we first note a useful fact about product states:

\[
\max_{\rho^i \ldots \rho^l} F(\rho, \rho_{A_1}^{I_1} \otimes \cdots \otimes \rho_{A_l}^{I_l}) = \max_{P_{RR' \rightarrow R_1 \ldots R_l}} \left| \langle \psi | R_1 C_1 \otimes \cdots \otimes \langle \psi |_{R_l C_l} P_{RR' \rightarrow R_1 \ldots R_l} |\psi\rangle_{RC} |0\rangle_{R'} \right|^2. \quad (33)
\]

In the case of a YES instance, the fidelity is guaranteed to be at least \((1 - \delta_c/2)^2 \geq 1 - \delta_c\) by the condition in (31) and the Fuchs-van-de-Graaf equality in (5). Thus, the prover can perform the \( P_{RR' \rightarrow R_1 \ldots R_l} \) that achieves this maximum. This gives probability at least \( 1 - \delta_c \) of accepting (the verifier should perform the \( l \) inverse unitaries and accept if he measures the all zero state on the output qubits).

In the case of a NO instance, the fidelity in (33) is no larger than \( 1 - \delta_s^2 / 4 \) by (32). Thus, it is impossible for the prover to perform any unitary \( P_{RR' \rightarrow R_1 \ldots R_l} \) that convinces the verifier to accept with probability greater than \( 1 - \delta_s^2 / 4 \). So, for an inverse polynomial gap \( \delta_s^2 / 4 - \delta_c \), there exists a \( \text{QSZK} \) proof system that decides \( \text{QPROD-STATE}(\delta_c, \delta_s) \).

To show \( \text{QSZK} \)-hardness, we can adapt the reduction used for \( \text{QSEP-STATE}_{1,1-\text{LOCC}} \) in [HMW13] by modifying it slightly to reduce \( \text{co-QSD} \) to \( \text{QPROD-STATE} \). Recall that for \( \text{co-QSD} \) [Wat02], we are given a description of circuits \( U_{\rho_0} \) and \( U_{\rho_1} \) that generate mixed states \( \rho_0 \) and \( \rho_1 \) on the system \( S \) as well as a reference system \( R \) that is traced over, and we are promised that either \( \| \rho_0 - \rho_1 \|_1 \leq \varepsilon \) in a YES instance or that \( \| \rho_0 - \rho_1 \|_1 \geq 2 - \varepsilon \) in a NO instance. As in the \( \text{QSEP-STATE}_{1,1-\text{LOCC}} \) reduction, let

\[
|\psi_{\rho_i}\rangle_{RS} \equiv U_{\rho_i} |0\rangle,
\]
Figure 7: Our QSZK proof system for deciding QPROD-STATE. The figure depicts the case in which the task is to decide if a general bipartite mixed state is product or not, but this easily extends to $l$-partite states (see the main text). The proof system begins with the verifier sending the reference system $R$ to the prover, who should be able to transform it into two separate purifications of each system of the original state. The verifier then performs the inverse of the original circuit on each pair $R_1 A_1$ and $R_2 A_2$ and measures to verify that the purifications sent by the prover are of the proper form. If the measurement outcomes are all zeros, then the verifier accepts that the original state is close to a product state and otherwise rejects.

Figure 8: Given respective circuit descriptions $U_{\rho_0}$ and $U_{\rho_1}$ for generating the states $\rho_0$ and $\rho_1$ on the output system $S$, one can compute a description for the above circuit in polynomial time. This serves both as a reduction from QUANTUM-STATE-DISTINGUISHABILITY to QSEP-STATE$_{1,1}$-LOCC and from co-QUANTUM-STATE-DISTINGUISHABILITY to QPROD-STATE by tracing out different systems in each case.
for \( i \in \{0, 1\} \) so that
\[
\rho_i = \text{Tr}_R\{|\psi_{\rho_i}\rangle\langle\psi_{\rho_i}|\}.
\]

From the description of the circuits \( U_{\rho_0} \) and \( U_{\rho_1} \), one can efficiently generate a description of the circuit in Figure 5 which takes as input a Bell state across the \( AB \) systems and performs the controlled unitary
\[
|0\rangle_B \otimes U_{\rho_0} + |1\rangle_B \otimes U_{\rho_1},
\]
to generate the state
\[
|\varphi\rangle_{ABRS} \equiv \frac{1}{\sqrt{2}} (|00\rangle_{AB} |\psi_{\rho_0}\rangle_{RS} + |11\rangle_{AB} |\psi_{\rho_1}\rangle_{RS}).
\]
The output qubits are divided into three sets: the qubits in the systems \( BR \) that are traced over, the half of a Bell state on system \( A \), and one of the states \( \rho_0 \) or \( \rho_1 \) on system \( S \). The resulting state after tracing out \( BR \) is
\[
\omega_{A:S} \equiv \text{Tr}_{BR}\{|\varphi\rangle\langle\varphi|_{ABRS}\}
= \frac{1}{2} (|0\rangle \otimes \rho_0 + |1\rangle \otimes \rho_1).
\]

In a YES instance, we wish to show that this state is close to product by giving a product state close to \( \omega_{A:S} \). To do this, we consider the state
\[
\sigma = \frac{1}{2} (|0\rangle \langle 0| + |1\rangle \langle 1|) \otimes \rho_0,
\]
for which the distance to \( \omega_{A:S} \) is given by:
\[
\|\omega_{A:S} - \sigma\|_1 = \frac{1}{2} \| |0\rangle \otimes \rho_0 + |1\rangle \otimes \rho_1 - |0\rangle \otimes \rho_0 - |1\rangle \otimes \rho_1\|_1
= \frac{1}{2} \| |1\rangle \otimes \rho_1 - |1\rangle \otimes \rho_0\|_1
= \frac{1}{2} \| \rho_1 - \rho_0\|_1
\leq \frac{\varepsilon}{2}.
\]

Thus, in a YES instance of co-QSD, our reduction results in a YES instance of QPROD-STATE with \( \delta_c = \frac{\varepsilon}{2} \).

In a NO instance, we must show that \( \omega_{A:S} \) is far from any product state. Recall that trace distance is equal to the maximum probability of distinguishing states over all possible measurements [Fuc96], so we can lower bound the distance to the nearest product state by considering a particular protocol to distinguish \( \omega_{A:S} \) from any product state. In this protocol, we begin by measuring the first qubit in the computational basis and by performing the Helstrom measurement \( \{\Pi_0, \Pi_1\} \) on the second qubit, storing the two measurement outcomes in classical registers.

It is straightforward to calculate the state \( \omega'_{A:S} \) that results after applying the protocol above to the state \( \omega_{A:S} \):
\[
\omega'_{A:S} = \frac{1}{2} \text{Tr}\{\Pi_0 \rho_0\} |00\rangle \langle 00| + \frac{1}{2} \text{Tr}\{\Pi_1 \rho_1\} |11\rangle \langle 11| + \frac{1}{2} \text{Tr}\{\Pi_0 \rho_1\} |10\rangle \langle 10| + \frac{1}{2} \text{Tr}\{\Pi_1 \rho_0\} |01\rangle \langle 01|.
\]
Recall that the Helstrom measurement distinguishes two states \( \rho_0 \) and \( \rho_1 \) with the following success probability:

\[
\frac{1}{2} \text{Tr}\{\Pi_0 \rho_0\} + \frac{1}{2} \text{Tr}\{\Pi_1 \rho_1\} = \frac{1}{2} \left( 1 + \frac{1}{2} \| \rho_0 - \rho_1 \|_1 \right),
\]

and the following error probability:

\[
\frac{1}{2} \text{Tr}\{\Pi_0 \rho_1\} + \frac{1}{2} \text{Tr}\{\Pi_1 \rho_0\} = \frac{1}{2} \left( 1 - \frac{1}{2} \| \rho_0 - \rho_1 \|_1 \right).
\]

Using this fact, it is straightforward to establish that the trace distance between \( \omega'_{A:S} \) and the perfectly correlated state \( \Phi_{A:S} \), defined as

\[
\Phi_{A:S} \equiv \frac{1}{2}(|00\rangle\langle00| + |11\rangle\langle11|),
\]

is no larger than

\[
1 - \frac{1}{2} \| \rho_0 - \rho_1 \|_1 \leq \frac{\epsilon}{2}.
\]

In the case of a product state, the two measurement outcomes must be uncorrelated, and so we can write the result of applying the above protocol to any product state using the probability \( p \) of measuring \( |0\rangle \langle0| \) and the probability \( q \) of measuring \( \Pi_0 \):

\[
\sigma_{p,q} = pq|00\rangle\langle00| + p(1 - q)|01\rangle\langle01| + q(1 - p)|10\rangle\langle10| + (1 - p)(1 - q)|11\rangle\langle11|.
\]

From the monotonocity of trace distance under quantum operations, it follows that

\[
\min_{\sigma_{0,\sigma_1}} \| \sigma_0 \otimes \sigma_1 - \omega_{A:S} \|_1 \geq \min_{p,q} \| \sigma_{p,q} - \omega'_{A:S} \|_1
\]

Due to symmetry, we can take \( p \leq \frac{1}{2} \) without loss of generality. We can then bound the minimum distance of \( \sigma_{p,q} \) to \( \omega'_{A:S} \):

\[
\min_{p,q} \| \sigma_{p,q} - \omega'_{A:S} \|_1 \geq \min_{p,q} \| \sigma_{p,q} - \Phi_{A:S} \|_1 - \| \Phi_{A:S} - \omega'_{A:S} \|_1
\]

\[
\geq \| \sigma_{p,q} - \Phi_{A:S} \|_1 - \frac{\epsilon}{2}
\]

\[
= \left| \frac{1}{2} - pq \right| + \left| \frac{1}{2} - (1 - p)(1 - q) \right| + |p(1 - q)| + |q(1 - p)| - \frac{\epsilon}{2}
\]

\[
= \frac{1}{2} - pq + \left| \frac{1}{2} - (1 - p)(1 - q) \right| + p(1 - q) + q(1 - p) - \frac{\epsilon}{2}
\]

\[
\geq \frac{1}{2} - pq + p(1 - q) + q(1 - p) - \frac{\epsilon}{2}
\]

\[
\geq \frac{1}{2} + p(1 - q) - \frac{\epsilon}{2}
\]

\[
\geq - \frac{\epsilon}{2},
\]

where the first line follows from the triangle inequality, and the fourth through last lines follow from the fact that \( 0 \leq p \leq \frac{1}{2} \) and \( 0 \leq q \leq 1 \). Thus in a NO instance of co-QSD, our reduction results in a NO instance of QPROD-STATE with \( \delta_s \geq (1 - \epsilon)/2 \).

We have given a QSZK proof system to decide QPROD-STATE, as well as a reduction from the QSZK-hard problem co-QSD. This completes the proof.
Remark 18 Theorem 17 constitutes a different proof that the promise problem known as Error Correctability from [HHT13] is QSZK-complete (with a proof preceding this one being given in [HST13]). Indeed, Error Correctability is the task of deciding whether it is possible to decode a maximally entangled state from systems $R$ and $B$ when a unitary specified as a quantum circuit acts on systems $R$, $B$, and $E$, such that systems $R$ and $B$ are initialized to the maximally entangled state and system $E$ is initialized to the all-zeros state. In this problem, there is a promise that it is either possible to decode maximal entanglement (approximately) or impossible to do so. Due to the “decoupling theorem” often used in quantum information theory [HHWY08], the question of whether it is possible to decode maximal entanglement between systems $R$ and $B$ is equivalent to the question of whether systems $R$ and $E$ are in a product state. Thus, it follows from Theorem 17 that Error Correctability and QPROD-STATE are reducible to one another and that Error Correctability is QSZK-complete.

8 A short quantum game for QSEP-STATE$_{1,1}$-

In Ref. [HMW13], it was shown that the QSEP-STATE$_{1,1}$-LOCC problem can be decided by a two-message quantum interactive proof system, so that the problem lies inside QIP(2). In this section, we show that this problem also admits a short quantum game, putting it inside SQG, too. As mentioned in Section 2, this result is not a complexity-theoretic improvement over prior work, but it is interesting that QSEP-STATE$_{1,1}$-LOCC admits a natural, single-message quantum proof provided that the verifier has help from a second competing prover.

Recall the multipartite definition of the QSEP-STATE$_{1,1}$-LOCC problem from Ref. [HMW13]:

Problem 19 (QSEP-STATE$_{1,1}$-LOCC($\delta_c, \delta_s$)) Given is a mixed-state quantum circuit to generate the $n$-qubit state $\rho_C$, along with a labeling of the qubits in the reference system $R$ and the output qubits for each system $A_1, A_2, \ldots, A_l \in C$. Decide whether

1. Yes: There is a separable state $\sigma_C \in S$ that is $\delta_c$-close in trace distance to $\rho_C$:
   \[
   \min_{\sigma_C \in S} \| \rho_C - \sigma_C \|_1 \leq \delta_c. 
   \] (34)

2. No: Every separable state is at least $\delta_s$-far in 1-LOCC distance to $\rho_C$:
   \[
   \min_{\sigma_C \in S} \| \rho_C - \sigma_C \|_{1-LOCC} \geq \delta_s. 
   \] (35)

Theorem 20 QSEP-STATE$_{1,1}$-LOCC($\delta_c, \delta_s$) is in SQG(c, s) for completeness $c = 1/2 - \delta_c/4$ and soundness $s = 1/2 - \delta_s/8$.

Proof. The short quantum game witnessing membership of QSEP-STATE$_{1,1}$-LOCC inside SQG(c, s) is as follows:

1. The yes-prover sends the verifier a state $\sigma_{C_1 \cdots C_k}$ where the number of systems $k$ is chosen to be
   \[
   k = \left\lceil t + \frac{16l^2 \log |C|}{\delta_s^2} \right\rceil. 
   \] (36)
   (Intuitively, the state $\sigma_{C_1 \cdots C_k}$ is a purported $k$-extension of $\rho_C$.)
2. The verifier performs a permutation test on the systems $C_1, \ldots, C_k$ received from the yes-prover in step 1. If the test fails, the verifier rejects. The verifier then discards all but one of the $k$ $C$ systems, leaving a state which we denote $\sigma_C = \text{Tr}_{C_2 \cdots C_k} \{ \sigma_{C_1} \cdots C_k \}$.

3. The verifier prepares a copy of the state $\rho_C$ using the input circuit and chooses a random bit $b \in \{0, 1\}$. If $b = 0$ he sends the no-prover the state $\rho_C$. Otherwise, he sends $\sigma_C$.

(Intuitively, the no-prover is challenged to identify whether the state he receives from the verifier is $\rho_C$ or $\sigma_C$.)

4. The no-prover replies with a single bit $b'$. The verifier rejects if and only if $b' = b$.

Let us argue that this protocol is correct. For YES instances, an optimal strategy for the yes-prover is to select a separable state $\sigma_C$ that is $\delta_c$-close in trace distance to $\rho_C$ and send the verifier a $k$-extension $\sigma_{C_1, \ldots, C_k}$ of $\sigma_C$. As $\sigma_C$ is separable, such a $k$-extension must exist for every choice of $k$ and so the permutation test passes with certainty. The no-prover is then faced with the task of distinguishing $\sigma_C$ from $\rho_C$, which he can do with probability no larger than $1/2 + \delta_c/4$, implying that the verifier accepts with probability at least $1/2 - \delta_c/4$ as desired.

For NO instances, an optimal strategy for the no-prover is to perform a measurement that distinguishes $\rho_C$ from the convex set $\mathcal{E}_k$ of $k$-extendable states with probability at least

\[ \frac{1}{2} + \frac{1}{4} \min_{\sigma_C \in \mathcal{E}_k} \| \rho_C - \sigma_C \|_1. \]  \hfill (37)

(The existence of such a measurement was first shown in Ref. [GW05] and a very simple proof can be found in Yu, Duan, and Xu [YDX12].)

To see that the yes-prover cannot win, observe that if the permutation test of step 2 passes, then the state $\sigma_{C_1, \ldots, C_k}$ received from the yes-prover is projected into each symmetric subspace of $C_{1, i} \cdots C_{k, i}$ (where $i$ indexes each party of the multipartite state). We know from Lemma 1 that choosing $k$ as in (36) given the condition (35) implies that

\[ \min_{\sigma_C \in \mathcal{E}_k} \| \rho_C - \sigma_C \|_1 \geq \delta_s/2. \]

It then follows from (37) and the fact that all states in such a symmetric subspace are contained in the set of permutation invariant states (the set of $k$-extendible states) that the no-prover convinces the verifier to reject with probability at least $1/2 + \delta_s/8$. This implies that the verifier accepts with probability at most $1/2 - \delta_s/8$ as desired. \[ \square \]

9 Prior Results

9.1 QSEP-STATE$_{1,1}$-LOCC and QIP(2)

**Problem 21 (QSEP-STATE$_{1,1}$-LOCC($\delta_c, \delta_s$))** Given is a mixed-state quantum circuit to generate the $n$-qubit state $\rho_{AB}$, along with a labeling of the qubits in the reference system $R$ and the output qubits for $A$ and $B$. Decide whether

1. Yes: There is a separable state $\sigma_{AB} \in \mathcal{S}$ such that $\rho_{AB}$ is $\delta_c$-close in trace distance to it:

\[ \min_{\sigma_{AB} \in \mathcal{S}} \| \rho_{AB} - \sigma_{AB} \|_1 \leq \delta_c. \]
Figure 9: A two-message quantum interactive proof system for \textit{QSEP-STATE}_{1,1-LOCC}. The proof system begins with the verifier executing the circuit $U_\rho$ that generates the state $\rho_C$. He sends the reference system to the prover. In the case that $\rho_C$ is fully separable, the prover should be able to act with a unitary on the reference system and some ancillas in order to generate a multipartite $k$-extension of $\rho_C$ to the systems $C_2$ through $C_k$. The prover sends all of the extension systems back to the verifier, who then performs phase estimation over the symmetric group (a quantum Fourier transform followed by a controlled permutation and measurement) in order to test if the state sent by the prover is a multipartite $k$-extension.

2. No: Every separable state is at least $\delta_s$-far in 1-LOCC distance to $\rho_{AB}$:

$$\min_{\sigma_{AB} \in S} \left\| \rho_{AB} - \sigma_{AB} \right\|_{1-LOCC} \geq \delta_s.$$ 

**Theorem 22** \textit{QSEP-STATE}_{1,1-LOCC}($\delta_c, \delta_s$) is \textit{NP}-hard (with respect to Cook reductions) and \textit{QSZK}-hard, and in \textit{QIP}(2) if there are polynomial-time computable functions $\delta_c, \delta_s : \mathbb{N} \rightarrow [0,1]$, such that the difference $\delta_s^2/8 - 2\sqrt{\delta_c}$ is larger than an inverse polynomial in the circuit size.

For a proof of this theorem refer to Sections 4-6 of [HMW13]. Section 8 of [HMW13] extends the theorem to the multipartite version. The \textit{QIP}(2) proof system is depicted in Figure 9.

9.2 \textit{QSEP-CHANNEL}_{1,1-LOCC} is \textit{QIP}-Complete

**Problem 23** (\textit{QSEP-CHANNEL}_{1,1-LOCC}($\delta_c, \delta_s$)) Given is a mixed-state quantum circuit to generate the channel $\mathcal{N}_{S \rightarrow AB}$, having an $n$-qubit input and an $m$-qubit output, along with a labeling of the qubits in the environment system $R$ and the output qubits for $A$ and $B$. Decide whether

1. Yes: There is an input to the channel $\rho_S$ such that the channel output $\mathcal{N}_{S \rightarrow AB}(\rho_S)$ is $\delta_c$-close in trace distance to a separable state $\sigma_{AB} \in S$:

$$\min_{\rho, \sigma_{AB} \in S} \left\| \mathcal{N}_{S \rightarrow AB}(\rho_S) - \sigma_{AB} \right\|_1 \leq \delta_c. \quad (38)$$

2. No: For every channel input $\rho_S$, the channel output $\mathcal{N}_{S \rightarrow AB}(\rho_S)$ is at least $\delta_s$-far in 1-LOCC distance to a separable state:

$$\min_{\rho, \sigma_{AB} \in S} \left\| \mathcal{N}_{S \rightarrow AB}(\rho_S) - \sigma_{AB} \right\|_{1-LOCC} \geq \delta_s.$$
Theorem 24 \textit{QSEP-CHANNEL}_{1,1-LOCC}(\delta_c, \delta_s) is QIP-complete if there are polynomial-time computable functions \( \delta_c, \delta_s : \mathbb{N} \rightarrow [0, 1] \) such that the difference \( \delta_s^2/8 - 2\sqrt{\delta_c} \) is larger than an inverse polynomial in the circuit size.

For a proof of this theorem refer to Section 7 of [HMW13]. The protocol can be extended to the multipartite case via the same method used to extend \textit{QSEP-STATE}_{1,1-LOCC}.

10 Operational interpretations of geometric measures of entanglement

Our work has a close connection to several entanglement measures known collectively as the geometric measure of entanglement (see [WG03, CAH13] and references therein). This is also the case with the work in [HM10], and we comment on this connection briefly.

The original definition of the geometric measure of entanglement was for a pure bipartite state \(|\psi\rangle_{AB}\) and defined in terms of the following quantity:

\[
\max_{|\phi\rangle_A, |\varphi\rangle_B} |\langle \phi \otimes \varphi | \psi \rangle_{AB}|^2. \tag{39}
\]

Clearly, this quantity has an operational interpretation as the maximum probability with which the state \(|\psi\rangle_{AB}\) would pass a test for being a pure product state. By taking the negative logarithm of this quantity, one recovers an entropic-like quantity that is equal to the geometric measure of entanglement and satisfies a list of desirable requirements that should hold for an entanglement measure. It is straightforward to extend the above definition and any of the ones below to the multipartite case.

If one has a promise that the quantity in (39) is larger or smaller than \(1 - \varepsilon\) or \(\varepsilon\), respectively, (as in our specification of \textit{QPROD-PURE-STATE}) then the product test and analysis of Harrow and Montanaro [HM10] demonstrate that it is easy to decide which is the case if one has access to a quantum computer. However, this does not directly give an operational interpretation to the quantity in (39). Rather, it is our QSZK proof system for \textit{QPROD-STATE} that has its maximum acceptance probability equal to the quantity in (39). More generally, this QSZK proof system has its maximum acceptance probability equal to a generalization of the quantity in (39) defined as follows for mixed states:

\[
\max_{\sigma_A, \omega_B} F(\rho_{AB}, \sigma_A \otimes \omega_B). \tag{40}
\]

As such, it gives a direct operational interpretation to the above quantity.

In prior work [HMW13], some of us demonstrated a QIP(2) proof system which had the following tight upper bound on its maximum acceptance probability:

\[
\max_{\sigma_{AB} \in S} F(\rho_{AB}, \sigma_{AB}), \tag{41}
\]

which holds in the limit of large \(k\), where \(k\) is the number of systems sent by the prover in a purported \(k\)-extension of the state \(\rho_{AB}\). The above quantity is again related to a geometric measure of entanglement defined in prior work (see [CAH13] and references therein). Thus, the QIP(2)-proof system for \textit{QSEP-STATE}_{1,1-LOCC} gives an operational interpretation to the quantity in (41) as the maximum probability with which a prover could convince a verifier that a state \(\rho_{AB}\) is separable if
the verifier sends a purification of $\rho_{AB}$ to the prover and then performs a check on what the prover sends back.

Finally, our work has unveiled and provided operational interpretations for other quantifiers of entanglement that fall within the geometric class. Indeed, the maximum acceptance probability for our proof system for $\text{QSEP-ISOMETRY}_{1,1}\text{-LOCC}$ is upper bounded by

$$\max_{\rho, \sigma_{AB} \in S} F(U(\rho_S \otimes |0\rangle\langle 0|)U^\dagger, \sigma_{AB}),$$

again a bound that holds in the large $k$ limit. Clearly, this quantity is related to the so-called “entangling power” of the unitary $U$ [ZZF00], that is, its ability to take a product state input to an entangled output no matter what the input is. Furthermore, the proof system for $\text{QSEP-CHANNEL}_{1,1}\text{-LOCC}$ given in [HMW13] has the following upper bound on its maximum acceptance probability:

$$\max_{\rho, \sigma_{AB} \in S} F(N_{S\rightarrow AB}(\rho_S), \sigma_{AB}),$$

where $N_{S\rightarrow AB}$ is a quantum channel with input system $S$ and output systems $AB$. Again, this bound holds in the limit of large $k$. The above measure is related to the entangling capabilities of a quantum channel no matter what the input is, and our proof system for $\text{QSEP-CHANNEL}_{1,1}\text{-LOCC}$ provides an operational interpretation for the above quantity as well.

11 Conclusion

We have proved that several entanglement or correlation detection problems are complete for BQP, QMA, QMA(2), and QSZK, building on prior work in [HMW13] that gives an entanglement detection promise problem in QIP(2) and a promise problem complete for QIP. The completeness of these promise problems for a wide range of complexity classes illustrates an important connection between entanglement and quantum computational complexity theory. In hindsight, it is perhaps natural that these problems related to entanglement can capture the expressive power of these classes since entanglement seems to be the most prominent feature which distinguishes classical from quantum computational complexity theory.

It is interesting to note the connection between these problems, and the differences that give rise to problems complete for different classes in the hierarchy. The differences are sometimes intuitive: a single-prover proof system for $\text{QSEP-ISOMETRY}$ would allow unentangled provers to be simulated with a single one, so, under the assumption that QMA is strictly contained in QMA(2), it seems natural that it should not be possible to place $\text{QSEP-ISOMETRY}$ in QMA. Some patterns between classes also emerge—it seems as though mixed state separability requires two messages to be added onto a proof system for pure state separability, in order to allow the prover to work with the purification of the mixed state (as is the case for both the “state” and “channel” versions of these problems).

Two-message quantum interactive proof systems continue to be somewhat mysterious. Intuitively, $\text{QSEP-STATE}_{1,1}\text{-LOCC}$ has the qualities that one would expect for a QIP(2)-complete problem by extrapolating from these results. Despite this, we do not know whether it is QIP(2)-complete or even QMA-hard. However, our work here gives evidence for why $\text{QSEP-STATE}_{1,1}\text{-LOCC}$ should not be either QSZK- or QMA-complete—there are are other problems very different from it that are complete for these classes ($\text{QPROD-STATE}$ and $\text{QPROD-ISOMETRY}$, respectively).
This work can be expanded in a number of directions. A trace-distance version of $\text{QSEP-CHANNEL}_{1,1}\text{-LOCC}$ may help to understand the relation between $\text{QMIP}$ and $\text{QMIP}_{\text{ne}}$, and similarly a trace-distance version of $\text{QSEP-STATE}_{1,1}\text{-LOCC}$ may provide further insights. Additionally, it would be worthwhile to characterize the channel version of $\text{QPROD-STATE}$ in order to map out more of the space of entanglement detection problems. Such an extension may also help to provide a tighter characterization of classes that rely on “unentanglement,” such as $\text{QMA}(2)$.

It is satisfying that each of the entanglement detection problems, with the exception of $\text{QSEP-STATE}_{1,1}\text{-LOCC}$, is complete for a different complexity class. Perhaps by visiting the remaining related problems in terms of the trace distance and mixed product state cases, one may find two different types of entanglement detection problems that are reducible to each other.

Acknowledgements

We thank Claude Cr´epeau and Brian Swingle for helpful conversations. KM acknowledges support from NSERC. PH is supported by the Canada Research Chairs program, the Perimeter Institute, CIFAR, NSERC and ONR through grant N000140811249. The Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. Some of this research was conducted while GG was a visitor at the School of Computer Science at McGill University, at which time GG’s primary affiliation was the Institute for Quantum Computing and School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada. GG was supported at that time by the Government of Canada through Industry Canada, the Province of Ontario through the Ministry of Research and Innovation, NSERC, DTO-ARO, CIFAR, and QuantumWorks. MMW began this project while affiliated with the School of Computer Science, McGill University and acknowledges support from the Centre de Recherches Mathématiques in Montreal.

A Appendix

A.1 Approximate $k$-extendibility

The following proposition applies to $l$-partite states $\rho_C = \rho_{A_1 \ldots A_l}$ that are approximately $k$-extendible:

**Proposition 25** Let $\rho_C$ be $\delta$-close to a $k$-extendible state, in the sense that

$$\min_{\sigma_C \in E_k} \|\rho_C - \sigma_C\|_1 \leq \delta,$$

for some $\delta > 0$, where $E_k$ is the set of $k$-extendible $l$-partite states. Then, the following bound holds

$$\|\rho_C - \mathcal{S}\|_{1\text{-LOCC}} \leq \sqrt{\frac{4l^2 \log|C|}{k-l}} + \delta$$

where the quantity on the left is multipartite 1-LOCC distance (defined in (7)) to the set of fully separable states.
Proof. Let $\sigma_C'$ be the state that achieves the minimum in (42). Since this state is $k$-extendible, we have from Theorem 2 of [BaH13] that

$$\min_{\sigma_C \in S} \|\sigma_C' - \sigma_C\|_{1-\text{LOCC}} \leq \sqrt{4l^2 \log |C| \over k - l},$$

(43)

Let $\sigma_C^*$ be the state achieving the minimum on the left in (43). From the premise of the theorem, it follows that

$$\|\sigma_C' - \sigma_C^*\|_1 - \text{LOCC} + \delta > \|\sigma_C' - \sigma_C^*\|_1 - \text{LOCC} + \|\sigma_C' - \rho_C\|_1$$

$$\geq \|\sigma_C' - \rho_C\|_1 - \text{LOCC}$$

$$\geq \min_{\sigma_C \in S} \|\sigma_C - \rho_C\|_1 - \text{LOCC}.$$

Thus,

$$\min_{\sigma_C \in S} \|\sigma_C - \rho_C\|_1 - \text{LOCC} < \|\sigma_C' - \sigma_C^*\|_1 - \text{LOCC} + \delta$$

$$\leq \sqrt{4l^2 \log |C| \over k - l} + \delta,$$

which concludes the proof. ■

A.2 Bounding pure state distance

Lemma 26 Given that

$$\min_{\rho, \sigma_{A_1 \cdots A_l} \in S} \|U(\rho_S \otimes |0\rangle\langle 0|)U^\dagger - \sigma_{A_1 \cdots A_l}\|_1 \leq \delta_c,$$

there exists a pure state $|\psi\rangle_s$ and a product state $|\phi_1\rangle \otimes \cdots \otimes |\phi_l\rangle$ such that

$$\|U(|\psi\rangle_s \otimes |0\rangle \langle 0| \otimes |0\rangle \otimes |0\rangle \otimes m)U^\dagger - |\phi_1\rangle_{A_1} \otimes \cdots \otimes |\phi_l\rangle_{A_l}\|_1 \leq 4\sqrt{\delta_c}.$$

(44)

The same is true if the minimization above is over the set of product states.

Proof. Since $\sigma_{A_1 \cdots A_l}$ is a separable state, it can be written in the following form:

$$\sigma_{A_1 \cdots A_l} = \sum_x p_X(x) |\phi_1^x\rangle_{A_1} \otimes \cdots \otimes |\phi_l^x\rangle_{A_l},$$

(The same is of course true for a product state.) Thus, a particular purification of $\sigma_{A_1 \cdots A_l}$ is the following state:

$$|\zeta\rangle_{RA_1 \cdots A_l} \equiv \sum_x \sqrt{p_X(x)} |x\rangle_R \otimes |\phi_1^x\rangle_{A_1} \otimes \cdots \otimes |\phi_l^x\rangle_{A_l}.$$

By Uhlmann’s theorem, we then know that there is a purification $|\psi\rangle_{RS}$ of $\rho_S$ such that the following condition holds

$$\|U(|\psi\rangle_{RS} \otimes |0\rangle \langle 0| \otimes |0\rangle \otimes m)U^\dagger - |\zeta\rangle_{RA_1 \cdots A_l}\|_1 \leq 2\sqrt{\delta_c}.$$  

(45)
We can then write $|\psi\rangle_{RS}$ as follows:

$$\sum_x \sqrt{q(x)}|x\rangle_R|\psi^x\rangle_S,$$

for some distribution $q(x)$ and states $\{|\psi^x\rangle\}$ (which are not necessarily orthonormal). Applying a dephasing in the basis $\{|x\rangle\}$ to the $R$ system of both states leading to the following inequality:

$$\left\| \sum_x q(x)|x\rangle_R \otimes |\psi^x\rangle_S \otimes |0\rangle^{\otimes m} \right\| U^\dagger - \sum_x p_X(x)|x\rangle_R \otimes |\phi^x_1\rangle_{A_1} \otimes \cdots \otimes |\phi^x_l\rangle_{A_l} \right\|_1 \leq 2\sqrt{\delta_c},$$

which follows by applying monotonicity of trace distance under noisy operations to (45). Tracing over the $A_1, \ldots, A_l$ systems then leads to

$$\|q - p_X\|_1 \leq 2\sqrt{\delta_c}.$$

We then find that

$$\left\| \sum_x p_X(x)|x\rangle_R \otimes \left[ U(|\psi^x\rangle_S \otimes |0\rangle^{\otimes m})U^\dagger - |\phi^x_1\rangle_{A_1} \otimes \cdots \otimes |\phi^x_l\rangle_{A_l} \right] \right\|_1 \leq \|q - p_X\|_1 + 2\sqrt{\delta_c} \leq 4\sqrt{\delta_c}.$$

This implies that

$$\sum_x p_X(x)\left\| U(|\psi^x\rangle_S \otimes |0\rangle^{\otimes m})U^\dagger - |\phi^x_1\rangle_{A_1} \otimes \cdots \otimes |\phi^x_l\rangle_{A_l} \right\|_1 \leq 4\sqrt{\delta_c},$$

from which we can conclude that the inequality is satisfied for at least one choice of $|\psi^x\rangle, |\phi^x_1\rangle \ldots |\phi^x_l\rangle$, implying (44).

**References**

[Aar13] Scott Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, March 2013.

[ABD+09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009. arXiv:0804.0802.
[Bab85] László Babai. Trading group theory for randomness. In Proceedings of the Seventeenth Annual ACM Symposium on the Theory of Computing, pages 421–429, 1985.

[BaC12] Fernando G. S. L. Brandão and Matthias Christandl. Detection of multiparticle entanglement: Quantifying the search for symmetric extensions. Physical Review Letters, 109:160502, October 2012. arXiv:1105.5720.

[BaH13] Fernando G. S. L. Brandão and Aram W. Harrow. Quantum de Finetti theorems under local measurements with applications. In Proceedings of the 45th annual ACM Symposium on the Theory of Computing, pages 861–870. ACM, 2013. arXiv:1210.6367.

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters, 70(13):1895–1899, March 1993.

[BBD+97] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. SIAM Journal on Computing, 26(5):1541–1557, October 1997. arXiv:quant-ph/9604028.

[BCY11] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. Communications in Mathematical Physics, 306:805–830, September 2011. arXiv:1010.1750.

[Bel64] John Stewart Bell. On the Einstein-Podolsky-Rosen paradox. Physics, 1:195–200, 1964.

[BM88] László Babai and Shlomo Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. Journal of Computer and System Sciences, 36(2):254–276, 1988.

[Boo12] Adam D. Bookatz. QMA-complete problems. 2012. arXiv:1212.6312.

[BSST99] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. Physical Review Letters, 83(15):3081–3084, October 1999. arXiv:quant-ph/9904023.

[BSST02] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. IEEE Transactions on Information Theory, 48:2637–2655, October 2002. arXiv:quant-ph/0106052.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, 69(20):2881–2884, November 1992.

[CAH13] Lin Chen, Martin Aulbach, and Michal Hajdusek. A comparison of old and new definitions of the geometric measure of entanglement. August 2013. arXiv:1308.0806.

[CB97] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. Physical Review A, 56(2):1201–1204, 1997.

37
[CHTW04] Richard Cleve, Peter Hoyer, Ben Toner, and John Watrous. Consequences and limits of nonlocal strategies. *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*, pages 236–249, June 2004. arXiv:quant-ph/0404076.

[CLMW10] Toby S. Cubitt, Debbie Leung, William Matthews, and Andreas Winter. Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104:230503, June 2010. arXiv:0911.5300.

[CN10] Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge University Press, 2010.

[Coo71] Stephen Cook. The complexity of theorem proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, pages 151–158, 1971.

[CS12] André Chailloux and Or Sattath. The complexity of the separable Hamiltonian problem. In *Proceedings of the 2012 IEEE Conference on Computational Complexity*, pages 32–41, Porto, Portugal, June 2012. arXiv:1111.5247.

[DPS02] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88:187904, April 2002. arXiv:quant-ph/0112007.

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69:022308, February 2004. arXiv:quant-ph/0308032.

[DPS05] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Detecting multipartite entanglement. *Physical Review A*, 71:032333, March 2005.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67(6):661–663, August 1991.

[Fuc96] Christopher A. Fuchs. Distinguishability and accessible information in quantum theory. 1996. arXiv:quant-ph/9601020.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45:1216, May 1999. arXiv:quant-ph/9712042.

[Gha10] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information and Computation*, 10(3):343–360, March 2010. arXiv:0810.4507.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. In *Proceedings of the Seventeenth Annual ACM Symposium on the Theory of Computing*, pages 291–304, 1985.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208, 1989.
[Gur03] Leonid Gurvits. Classical deterministic complexity of Edmonds’ problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 10–19, June 2003. arXiv:quant-ph/0303055.

[GW05] Gus Gutoski and John Watrous. Quantum interactive proofs with competing provers. In *Proceedings of the 22nd Symposium on Theoretical Aspects of Computer Science*, volume 3404 of *Lecture Notes in Computer Science*, pages 605–616, 2005. arXiv:cs/0412102 [cs.CC].

[GW13] Gus Gutoski and Xiaodi Wu. Parallel approximation of min-max problems. *Computational Complexity*, 22(2):1–44, 2013. arXiv:1011.2787.

[Hel69] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, June 1969.

[Hel76] Carl W. Helstrom. *Quantum Detection and Estimation Theory*. Academic, New York, 1976.

[HH13] Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. January 2013. arXiv:1301.4504.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865–942, June 2009. arXiv:quant-ph/0702225.

[HHWy08] Patrick Hayden, Michal Horodecki, Andreas Winter, and Jon Yard. A decoupling approach to the quantum capacity. *Open Systems & Information Dynamics*, 15:7–19, March 2008. arXiv:quant-ph/0702005.

[HM10] Aram Harrow and Ashley Montanaro. An efficient test for product states with applications to quantum Merlin-Arthur games. In *Proceedings of the 51st Annual IEEE Symposium on the Foundations of Computer Science (FOCS)*, pages 633–642, 2010. arXiv:1001.0017.

[HMW13] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. In *Proceedings of the 18th Annual IEEE Conference on Computational Complexity*, pages 156–167, 2013. arXiv:1211.6120.

[Hol72] Alexander S. Holevo. An analog of the theory of statistical decisions in noncommutative theory of probability. *Trudy Moscov Mat. Obsc.*, 26:133–149, 1972. English translation: Trans. Moscow Math Soc. 26, 133–149 (1972).

[HS12] Patrick Hayden and Brian Swingle. Quantum error correction and QSZK. unpublished, 2012.

[JJuW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Communications of the ACM*, 53(12):102–109, December 2010. arXiv:0905.1300.

[JuW09] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. *50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543, October 2009. arXiv:0905.1300.
[Kit95] Alexei Kitaev. Quantum measurements and the abelian stabilizer problem. November 1995. arXiv:quant-ph/9511026.

[Kit99] Alexei Kitaev. Quantum NP. Talk at the 2nd Workshop on Algorithms in Quantum Information Processing, DePaul University, Chicago, January 1999.

[KKR06] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006. arXiv:quant-ph/0406180.

[KMY01] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum certificate verification: Single versus multiple quantum certificates. 2001. arXiv:quant-ph/0110006.

[KNY08] Masaru Kada, Harumichi Nishimura, and Tomoyuki Yamakami. The efficiency of quantum identity testing of multiple states. *Journal of Physics A: Mathematical and Theoretical*, 41(39):395309, October 2008. arXiv:0809.2037.

[KŠV02] Alexei Y. Kitaev, Alexander H. Šen, and Mikhail N. Vyalyi. *Classical and quantum computation*. Number 47. American Mathematical Society, 2002.

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 608–617, May 2000.

[LW12] Cécilia Lancien and Andreas Winter. Distinguishing multi-partite states by local measurements. June 2012. arXiv:1206.2884.

[MCKB05] Florian Mintert, André R.R. Carvalho, Marek Kuś, and Andreas Buchleitner. Measures and dynamics of entangled states. *Physics Reports*, 415(4):207–259, 2005. arXiv:quant-ph/0505162.

[MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. arXiv:cs/0506068.

[MWW09] William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, November 2009. arXiv:0810.2327.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NWZ09] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information & Computation*, 9(11):1053–1068, 2009. arXiv:0904.1549.

[Pap94] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994. Theorem 16.3.

[Ros11] Bill Rosgen. Testing non-isometry is QMA-complete. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 63–76. Springer, 2011. arXiv:0910.3740.
[Sip96] Michael Sipser. *Introduction to the Theory of Computation*. International Thomson Publishing, 1996.

[Sto76] Larry J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3(1):1–22, 1976.

[Uhl76] Armin Uhlmann. The “transition probability” in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[VV12] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. October 2012. arXiv:1210.1810.

[Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 537–546, 2000. arXiv:cs/0009002.

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468, November 2002. arXiv:quant-ph/0202111.

[Wat03] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, January 2003.

[Wat04] John Watrous. Lecture 17: LOCC distinguishability of sets of states. *Theory of Quantum Information* (course lecture notes), 2004.

[Wat09a] John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and System Science*, 2009. arXiv:0804.3401.

[Wat09b] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. arXiv:quant-ph/0511020.

[Wer89a] Reinhard F. Werner. An application of Bell’s inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17:359–363, 1989.

[Wer89b] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277–4281, October 1989.

[WG03] Tzu-Chieh Wei and Paul M. Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Physical Review A*, 68:042307, October 2003. arXiv:quant-ph/0307219.

[Wil11] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. 2011. arXiv:1106.1445.

[Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[YDX12] Nengkun Yu, Runyao Duan, and Quanhua Xu. Bounds on the distance between a unital quantum channel and the convex hull of unitary channels, with applications to the asymptotic quantum Birkhoff conjecture. arXiv:1201.1172 [quant-ph], January 2012.
[ZZF00] Paolo Zanardi, Christof Zalka, and Lara Faoro. Entangling power of quantum evolutions. *Physical Review A*, 62:030301, August 2000. arXiv:quant-ph/0005031.