THEORY OF COMPUTING, Volume 11 (3), 2015, pp. 59–103
www.theoryofcomputing.org

Quantum Interactive Proofs and the Complexity of Separability Testing

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

Received September 8, 2013; Revised January 27, 2015; Published March 26, 2015

Abstract: We identify a formal connection between physical problems related to the detection of separable (unentangled) quantum states 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), and QSZK), there corresponds a natural separability testing problem that is complete for that class. Of particular interest is the fact that the problem of determining whether an isometry can be made to produce a separable state is either QMA-complete or QMA(2)-complete, depending upon whether the distance between quantum states is measured by the one-way LOCC norm or the trace norm. We obtain strong hardness results by employing prior work on entanglement purification protocols to prove that for each n-qubit maximally entangled state there exists a fixed one-way LOCC measurement that distinguishes it from any separable state with error probability that decays exponentially in n.

ACM Classification: F.1.3

AMS Classification: 68Q10, 68Q15, 68Q17, 81P68

Key words and phrases: quantum entanglement, quantum complexity theory, quantum interactive proofs, quantum statistical zero knowledge, BQP, QMA, QSZK, QIP, separability testing

*Supported by Government of Canada through Industry Canada, the Province of Ontario through the Ministry of Research and Innovation, NSERC, DTO-ARO, CIFAR, and QuantumWorks.

†Supported by 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.

‡Supported by NSERC.

§Supported by Centre de Recherches Mathématiques.

DOI: 10.4086/toc.2015.v011a003

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 [68] all the way up to PSPACE [67], 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.[1] Likewise, in the domain of interactive proofs [4, 38, 5, 71, 54, 73], 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 information [49], including quantum teleportation [9], super-dense coding [13], enhanced communication capacities [11, 12, 28], device-independent quantum key distribution [35, 69], and communication complexity [25]. Thus, deciding whether a given quantum state is separable (unentangled) or entangled 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 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 [39, 37].

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 (as in a quantum circuit) or the application of a local Hamiltonian [59, 14]. This formulation of the quantum separability problem was studied by three of us [46], wherein it was shown that the problem is hard for both QSZK and NP, even when one demands that no-instances be far from separable in the so-called "one-way LOCC distance" (and not merely in trace distance). It was also shown that this one-way LOCC variant of the problem admits a two-message quantum interactive proof, putting it in $\mathsf{QIP}(2)$. The exact complexity of this problem is still open.

Informally, the *one-way LOCC distance* is an operationally motivated distance measure for bipartite quantum states [62]. Given two states ρ, ξ of registers AB, the one-way LOCC norm $\|\rho - \xi\|_{\text{1-LOCC}}$ dictates the maximum probability with which ρ could be distinguished from ξ by two parties acting locally on registers A, B and endowed with classical communication from A to B. It is clear that the one-way LOCC distance is no larger than the trace distance, and it can sometimes be much smaller [34, 29, 30, 62]. In one of the earliest examples [34], it was found that maximally mixed states on the symmetric and antisymmetric subspace of two systems of dimension d have a 1-LOCC distance no larger than $O(1/d)$ while their trace distance is maximal, given that these states are orthogonal. See Section 2.4 for details.

In this paper, we explore several variations on the complexity of determining whether a state specified by a quantum circuit is separable, or whether a channel specified by a quantum circuit can be made to produce a separable output state. The properties we vary include the following:

[1] For 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 [64, Ch. 4.2, Theorem 16.3], while if one allows only Horn clauses the resulting problem (HORNSAT) is P-complete [27], and if one removes any such limitations on clauses the problem (SAT) is NP-complete [26].

1. Allowing arbitrary mixed states versus restricting attention to pure states.

2. Allowing arbitrary channels versus restricting attention to isometric channels.

3. We 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).

4. Measuring distance between quantum states using the trace norm or the so-called "one-way LOCC norm" of [62].

We study seven different combinations of these properties, obtaining problems that are complete for four different complexity classes based on quantum interactive proofs: BQP, QMA, QMA(2), and QSZK. Our study applies to multipartite states and channels, though only bipartite states and channels are required for the hardness results. We obtain strong hardness results as a corollary of a theorem establishing the existence of a fixed one-way LOCC measurement that successfully distinguishes a given n-qubit maximally entangled state from any separable state with error probability that decays exponentially in n. (Theorem 3.1 of Section 3.) It appears that this observation has not yet been made explicitly in the literature, though it is implied by prior results on entanglement purification protocols [10, 7, 3, 43]. We provide a new proof.

Outline of paper. A detailed list of our complexity theoretic results is given in Figure 1 of Section 1.1. A summary of relevant concepts such as the one-way LOCC distance, various complexity classes, the permutation and swap tests is given in Section 2. Our strong lower bound on the one-way LOCC distance between maximally entangled and separable states is proven in Section 3. The completeness results are presented in Sections 4–7. In Section 9 we discuss how these completeness results provide operational interpretations for several geometric measures of entanglement discussed in [75, 23] and references therein. Finally, we conclude in Section 11 with a summary of our results and a discussion of directions for future research.

1.1 Overview of results

Figure 1 gives a brief description of each problem and provides a concise summary of our results. Below we give more details of our results along with their relation to prior results in the literature:

1. PURE PRODUCT STATE is BQP-complete, as is the one-way LOCC version of the problem. (Theorem 4.2 of Section 4.) Membership in BQP follows from the soundness of the "product test" [44]. Hardness of the one-way LOCC version follows from an application of Theorem 3.1.

2. The one-way LOCC version of SEPARABLE ISOMETRY OUTPUT is QMA-complete. (Theorem 5.2 of Section 5.) Membership in QMA follows from the existence of succinct k-extendible witnesses for separability [17]. (A similar approach was used in previous work by three of us to place the one-way LOCC version of SEPARABLE STATE inside QIP(2) [**?**, 46].) Hardness follows from another application of Theorem 3.1.

3. PURE PRODUCT ISOMETRY OUTPUT, PRODUCT ISOMETRY OUTPUT, and SEPARABLE ISOMETRY OUTPUT are QMA(2)-complete. (Theorem 6.2 and Corollary 6.9 of Section 6.) Membership of PURE PRODUCT ISOMETRY OUTPUT in QMA(2) follows from a simple application of the swap test combined with the collapse $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ [44]. Hardness is the result of a novel circuit gadget (Figure 4). Completeness for the other two problems follows by an equivalence to PURE PRODUCT ISOMETRY (Section 6.3).

4. PRODUCT STATE is QSZK-complete. (Theorem 7.2 of Section 7.) The result follows by an equivalence with the QSZK-complete problem QUANTUM STATE SIMILARITY [70, 74].

5. The one-way LOCC version of SEPARABLE STATE is in SQG, a competing-provers class known to coincide with PSPACE [41]. (Proposition 8.2 of Section 8.) As mentioned previously, this problem is already known to be contained in QIP(2) [46], which is a subset of PSPACE [51, 50]. Thus, this new bound is not a complexity-theoretic improvement over prior work.

   However, it is interesting that this problem admits a succinct quantum witness in support of separability, 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 of [46] depends critically upon the ability of the prover to apply a *channel* in support of separability.

2 Preliminaries

This section summarizes some facts about quantum information and complexity theory relevant for the rest of the paper. Familiarity with both fields of study is assumed; our primary goal here is to establish notation and terminology. Some references giving background on these topics are [63, 78, 79] and [73, 1].

2.1 Registers, states, separable states

A *register* is a finite-level quantum system, which is implicitly identified with a finite-dimensional complex Euclidean space. Registers are denoted with Roman capital letters $A, B, \ldots$. The *state* of a register is described by a *density matrix*, which is a positive semidefinite matrix ρ with $\operatorname{Tr}(\rho) = 1$. A *pure state* is a rank-one density matrix. Pure states can be written in standard bra-ket notation $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle$. It is common practice to refer to unit vectors $|\psi\rangle$ as pure states. The Greek letters ϕ, ψ are reserved for pure states and we often abbreviate $|\psi\rangle\langle\psi|$ to ψ.

A multipartite state $\rho_{A_1 \cdots A_l}$ is a *product state* if $\rho_{A_1 \cdots A_l} = \rho_{A_1} \otimes \cdots \otimes \rho_{A_l}$ for states $\rho_{A_1}, \ldots, \rho_{A_l}$ of registers $A_1, \ldots, A_l$, respectively. A state is *separable* if it can be written as a probabilistic mixture of product states [77]. That is, a multipartite state $\rho_{A_1 \cdots A_l}$ is said to be *separable* if it admits a decomposition of the following form:

$$\rho_{A_1 \cdots A_l} = \sum_{y \in \mathcal{Y}} p_Y(y)\, \sigma_{A_1}^{1,y} \otimes \cdots \otimes \sigma_{A_l}^{l,y}, \tag{2.1}$$

for collections $\{\sigma_{A_1}^{1,y}\}, \ldots, \{\sigma_{A_l}^{l,y}\}$ of quantum states and some probability distribution $p_Y(y)$ over an alphabet $\mathcal{Y}$ [77]. By applying the spectral theorem to each density operator, we can always find a

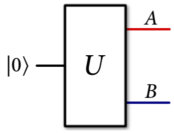
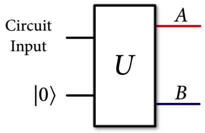
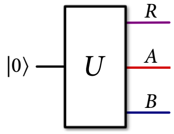
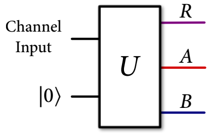
Problem name	Description	Complexity	Circuit
• Pure Product State • Pure Product State, one-way LOCC version	Is the state generated by the pure-state quantum circuit close to a product state?	BQP-complete	
• Separable Isometry Output, one-way LOCC version	Is there an input to the isometry such that the output is close to a separable state in trace distance, or does every input lead to an output that is far from separable in one-way LOCC distance?	QMA-complete	
• Pure Product Isometry Output • Product Isometry Output • Separable Isometry Output	Is there an input to the isometry such that the output is close to a product/separable state?	QMA(2)-complete	
• Product State	Is the state generated by the mixed-state circuit close to a product state?	QSZK-complete	
• Separable State, one-way LOCC version	Is the state generated by the mixed-state circuit close to a separable state?	In QIP(2). QSZK-hard, NP-hard. [46]	
• Separable Channel Output, one-way LOCC version	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 one-way LOCC distance?	QIP-complete [46]	

Figure 1: The collected results of separability testing problems and their complexity. A "one-way LOCC version" of a problem means that distances for yes-instances are measured by the trace norm, but distances for no-instances are measured by the one-way LOCC norm.

decomposition of any separable state in terms of pure product states:

$$\rho_{A_1\cdots A_\ell} = \sum_{z\in\mathcal{Z}} p_Z(z)\,|\psi^{1,z}\rangle\langle\psi^{1,z}|_{A_1}\otimes\cdots\otimes|\psi^{\ell,z}\rangle\langle\psi^{\ell,z}|_{A_\ell}\,. \tag{2.2}$$

A state is *entangled* if it is not separable.

In the multipartite case it is often necessary to specify the *cut* or *partition* of the registers relative to which ρ is product or separable. For example, a state ρ of registers $ABCD$ could be a bipartite product state with respect to the cut $AB:CD$, yet it may not be a product state with respect to the tripartite cut $A:B:CD$ or the bipartite cut $AC:BD$. We let $\mathcal{S}$ denote the set of all separable states with respect to a given cut. Whenever the cut is not immediately clear from the context, we make it explicit with an argument—for example, $\mathcal{S}(A:B:CD)$.

2.2 Trace distance, fidelity

The *Schatten 1-norm* $\|X\|_1$ of a matrix X is defined as the sum of the singular values of X. (Hereafter we refer to this norm as simply the *1-norm*. This norm is sometimes called the *trace norm* and is alternately denoted $\|X\|_{\mathrm{Tr}}$.) The 1-norm characterizes the physically observable difference between two quantum states ρ,ξ in the following sense: given a quantum register prepared in one of $\{\rho,\xi\}$ chosen uniformly at random, the maximum probability with which one can correctly identify the given state by a two-outcome measurement of that register is equal to $1/2+\|\rho-\xi\|_1/4$. The measurement that achieves this maximal probability is known as the *Helstrom measurement* [48].

The quantity $\|\rho-\xi\|_1$ is sometimes called the *trace distance* between ρ,ξ. The trace distance between two quantum states ρ,ξ is given by the following variational characterization:

$$\|\rho-\xi\|_1 = 2\max_{0\preceq\Pi\preceq I}\mathrm{Tr}(\Pi(\rho-\xi))\,, \tag{2.3}$$

where the maximizing $\Pi^\star$ leads to the Helstrom measurement $\{\Pi^\star, I-\Pi^\star\}$. A straightforward consequence of (2.3) is that if two states are close in trace distance then they must have similar measurement statistics. In particular, for all measurement operators $0\preceq\Pi\preceq I$ it holds that

$$\mathrm{Tr}(\Pi\rho)\geq\mathrm{Tr}(\Pi\xi)-\frac{1}{2}\|\rho-\xi\|_1\,. \tag{2.4}$$

The trace distance $\|\psi-\phi\|_1$ between two pure states $|\psi\rangle,|\phi\rangle$ is related to the inner product $\langle\psi|\phi\rangle$ by the formula

$$|\langle\phi|\psi\rangle|^2 = 1-\|\psi-\phi\|_1^2/4\,. \tag{2.5}$$

The following implication holds for any pure states ϕ,ψ and any $\varepsilon\in[0,1]$:

$$|\langle\phi|\psi\rangle|^2\geq 1-\varepsilon \implies \|\phi-\psi\|_1\leq 2\sqrt{\varepsilon}\,. \tag{2.6}$$

The *fidelity* is a pseudodistance measure for quantum states given by

$$F(\rho,\xi) = \left\|\sqrt{\rho}\sqrt{\xi}\right\|_1^2 \tag{2.7}$$

for all density matrices ρ,ξ. *Uhlmann's Theorem* asserts that the fidelity between two states ρ,ξ is the optimal squared overlap between purifications of ρ,ξ:

$$F(\rho,\xi)=\max_{|\phi_\rho\rangle,|\phi_\sigma\rangle}|\langle\phi_\rho|\phi_\sigma\rangle|^2. \tag{2.8}$$

Uhlmann's Theorem gives the fidelity an operational interpretation as the maximum probability with which a purification of ρ would pass a test for being a purification of σ. The fidelity and trace distance are related by the Fuchs-van-de-Graaf inequalities [36]:

$$1-\sqrt{F(\rho,\xi)}\leq\frac{1}{2}\|\rho-\xi\|_1\leq\sqrt{1-F(\rho,\xi)}. \tag{2.9}$$

2.3 Permutation test, swap test

The *permutation test* is a quantum circuit applied to a multi-register system $A_1,\ldots,A_n$ with the property that the probability of passing is equal to the shadow of the state on the symmetric subspace of the complex Euclidean space associated with $A_1,\ldots,A_n$ (i. e., $\mathrm{Tr}(\Pi^{\mathrm{sym}}_{A_1,\ldots,A_n}\rho)$) [53] (see also [6, 52]). Furthermore, if the test passes, then the resulting state of those registers is supported on the symmetric subspace. The test consists of the following steps:

1. Prepare an $n!$-dimensional ancillary register W in a uniform superposition of all $n!$ computational basis states. (This is accomplished by applying the quantum Fourier transform to the all-zeros state $|0\rangle$ of W.)

2. Apply a controlled-permutation unitary that permutes registers $A_1,\ldots,A_n$ according to the permutation indexed in register W.

3. Invert the quantum Fourier transform on W and measure that register in the computational basis. Accept if and only if the measurement outcome is all zeros.

A special case of the permutation test for $n=2$ is known as the *swap test* [20]. (In this case the ancillary register W is just a single qubit and the quantum Fourier transform is just the standard Hadamard gate.) The swap test has the powerful property that if registers A_1A_2 are prepared in a pure product state $|\psi\rangle|\phi\rangle$ then the swap test passes with probability

$$\frac{1}{2}+\frac{1}{2}|\langle\psi|\phi\rangle|^2=1-\frac{1}{8}\|\psi-\phi\|_1^2. \tag{2.10}$$

Thus, with repetition, the swap test can be used to estimate the distance between any two unknown pure states.

2.4 One-way LOCC distance

In this paper we are sometimes interested in the distinguishability of multipartite quantum states under the restriction that the distinguishing measurement must be implementable by local operations with unidirectional classical communication. This class of measurements induces a matrix norm called the *one-way LOCC norm* [62]. For each matrix X acting on the complex Euclidean space associated with registers AB, the one-way LOCC norm $\|X\|_{\text{1-LOCC}}$ of X is defined by

$$\|X\|_{\text{1-LOCC}} = \max_{\Lambda_{B\to M}} \|(I_A \otimes \Lambda_{B\to M})(X)\|_1 , \tag{2.11}$$

where the maximization is over all *quantum-to-classical* channels $\Lambda_{B\to M}$. These are the channels that measure the contents of register B and store the classical outcome in a new register M. Every such channel has the form

$$\Lambda_{B\to M}(\rho) = \sum_m \mathrm{Tr}(\Lambda_m \rho)|m\rangle\langle m| , \tag{2.12}$$

where $\{|m\rangle\}$ is an orthonormal basis and $\{\Lambda_m\}$ forms a quantum measurement, meaning that each Λ_m is positive semidefinite and $\sum_m \Lambda_m = I$.

This definition of the one-way LOCC norm is asymmetric: one could define another norm as a maximization over measurements of register A, and these norms are distinct. It is clear from the definition that

$$\|X\|_{\text{1-LOCC}} \leq \|X\|_1 , \tag{2.13}$$

because the one-way LOCC measurements are a subset of all measurements.

The one-way LOCC norm extends naturally to multi-register systems [56, 16, 19]. In particular, for each matrix X acting on the complex Euclidean space associated with registers $A_1 \cdots A_\ell$, the ℓ-partite one-way LOCC norm of X is given by

$$\|X\|_{\text{1-LOCC}} = \max_{\Lambda_{A_2},\dots,\Lambda_{A_\ell}} \|(I_{A_1} \otimes \Lambda_{A_2} \otimes \cdots \otimes \Lambda_{A_\ell})(X)\|_1 , \tag{2.14}$$

where the maximization is now over quantum-to-classical channels $\Lambda_{A_2},\dots,\Lambda_{A_l}$. The interpretation here when X is a difference of two density matrices is that the last $\ell - 1$ parties each perform a local measurement on their systems and communicate the results to the first party, who then attempts to distinguish the two states.

2.5 Quantum interactive proofs

A *quantum interactive proof* consists of a conversation between a polynomial-time quantum *verifier* and a computationally unbounded quantum *prover* regarding some binary input string x. The prover attempts to convince the verifier to accept x and the verifier attempts to judge the veracity of the prover's argument. A promise problem L is said to admit a quantum interactive proof with *completeness* c and *soundness* s if there exists $c, s \in [0, 1]$ such that $c > s$ and a verifier who meets the following conditions:

Completeness condition. If x is a yes-instance of L, then the prover can convince the verifier to accept with probability at least c.

Soundness condition. If x is a no-instance of L, then no prover can convince the verifier to accept with probability higher than s.

The completeness and soundness parameters c,s need not be fixed constants but may instead vary as a function of the input length $|x|$. If these parameters are not specified then it is assumed that L admits a quantum interactive proof for some choice of $c(|x|),s(|x|)$ for which there exists a polynomial-bounded function $p(|x|)$ such that $c-s \geq 1/p$. The complexity class QIP consists of all promise problems that admit quantum interactive proofs and is known to coincide with PSPACE [50].

Often in the study of interactive proofs the precise values of c,s are immaterial because error-reduction procedures can be used to transform any verifier for which $c-s \geq 1/p$ into another verifier for which c tends toward one and s tends toward zero exponentially quickly in the bit length of x. (For example, sequential repetition followed by a majority vote can be used to reduce error for QIP.) For this reason, it is typical to assume without loss of generality that c,s are constants such as $2/3, 1/3$ or that c is exponentially close to one and s is exponentially close to zero whenever it is convenient to do so. However, it is not always clear that a given complexity class is robust with respect to the choice of c,s so it is good practice to be as inclusive as possible when defining these classes.

Interesting subclasses of QIP are obtained by restricting the number of messages in the interaction between the verifier and prover. For each positive integer m, the class $\mathsf{QIP}(m)$ consists of those problems that admit a quantum interactive proof in which the verifier exchanges no more than m messages with the prover. It is known that three messages suffice for any quantum interactive proof, so that $\mathsf{QIP} = \mathsf{QIP}(3)$ [54], leaving a hierarchy of four classes defined by quantum interactive proofs. Fundamental complexity classes such as BQP and QMA can be written in this notation as $\mathsf{QIP}(0)$ and $\mathsf{QIP}(1)$, respectively. This hierarchy, along with other complexity classes considered in this paper (other than $\mathsf{QMIP}_{\mathrm{ne}}$), is depicted in Figure 2. $\mathsf{QMIP}_{\mathrm{ne}}$ is a class defined in [55]—it allows for multiple prover interactive proofs with provers who do not share entanglement (clearly, this contains both $\mathsf{QMA}(2)$ and QIP).

A quantum interactive proof for a promise problem L is said to be *statistical zero knowledge* if for each yes-instance x of L the verifier learns nothing from the prover beyond the veracity of the claim "x is a yes-instance of L." This property is formalized via a simulation-based definition of "knowledge." The complexity class of promise problems that admit statistical zero knowledge quantum interactive proofs is called QSZK. We need not concern ourselves with a precise definition of this class, since our completeness results are established by equivalence to another QSZK-complete problem. The reader is referred to the seminal works in [70, 74] for more information on statistical zero knowledge quantum interactive proofs.

Other interesting variations of the quantum interactive proof model are obtained by considering multiple cooperating or competing provers. For example, one can consider a variant of QMA in which k distinct and unentangled provers cooperate in order to convince the verifier to accept. The resulting complexity class is called $\mathsf{QMA}(k)$ and is known to satisfy $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ for all integers $k \geq 2$ [44]. The only known bounds for $\mathsf{QMA}(2)$ are the trivial bounds $\mathsf{QMA} \subseteq \mathsf{QMA}(2) \subseteq \mathsf{NEXP}$. Lower bounds for $\mathsf{QMA}(2)$ are presented in references [2, 15, 8, 22, 57, 24]; upper bounds in references [18, 66].

Despite the lack of any decent upper bound on $\mathsf{QMA}(2)$, we are aware of only two problems in $\mathsf{QMA}(2)$ that are not also known to be in QMA: the pure-state N-representability problem [58] and the separable sparse Hamiltonian problem [21]. Of these, only the latter is known to be $\mathsf{QMA}(2)$-complete. The present paper gives another $\mathsf{QMA}(2)$-complete problem in Section 6.

Alternately, one could consider quantum interactive proofs with two competing provers: one prover—the *yes-prover*—tries to convince the verifier to accept x while the other prover—the *no-prover*—tries

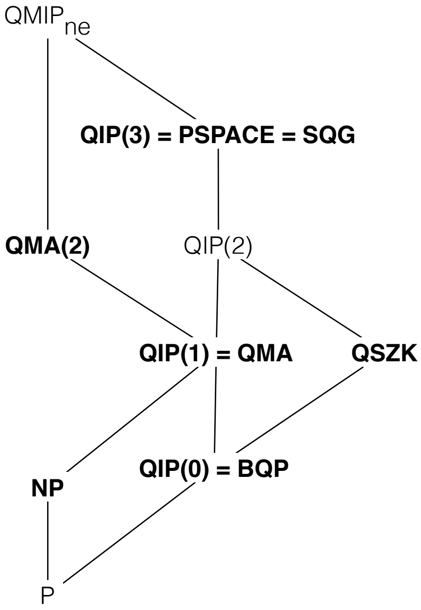


Figure 2: The quantum interactive proof hierarchy and related classes discussed in this paper. A line denotes inclusion of the lower class in the higher class. (For example, P is a subset of NP.) Classes for which a separability testing problem is known to be complete are in bold type.

to convince the verifier to reject x. As before, interesting complexity classes are obtained by restricting the number and timing of messages in the interaction between the verifier and provers. In Section 8 we exhibit a protocol in which the verifier receives a single message from the yes-prover and then exchanges two messages with the no-prover. The complexity class of promise problems that admit such proofs is called SQG (for "short quantum games") and is known to coincide with PSPACE [41].

Each of the aforementioned complexity classes 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. Error reduction for BQP follows immediately from Chernoff-type bounds via sequential repetition followed by a majority vote. Error-reduction results for QIP, QIP(2), QMA, QSZK, QMA(2), and SQG were established in [54, 51, 61, 70, 44, 41], respectively.[2]

[2] That SQG is robust with respect to error follows from the containments $\mathsf{SQG}(c,s) \subseteq \mathsf{PSPACE}$ for any $c - s > 1/\text{poly}$ [41] and $\mathsf{PSPACE} \subseteq \mathsf{SQG}(1-\varepsilon, \varepsilon)$ for any desired exponentially small ε [40]. However, the "error reduction procedure" induced here is very circuitous: a high-error short quantum game must be simulated in polynomial space, and then that polynomial-space computation must be converted back into a low-error short quantum game via proofs of $\mathsf{IP} = \mathsf{PSPACE}$ [60, 65]. It is not known whether a more straightforward transformation such as parallel repetition followed by a majority vote could be used to reduce error for SQG.

3 One-way LOCC distance to a separable state

In this section we prove a theorem that enables us to establish strong hardness results for various separability testing problems appearing later in the paper.

If $|\phi\rangle$ is any maximally entangled pure state of two n-qubit registers AB then

$$\max_{\sigma \in \mathcal{S}(A:B)} F(\phi,\sigma) = 2^{-n}. \tag{3.1}$$

A concise proof of the above equality can be found in [72, Lecture 17]. Applying the above relation and (2.9), we find the following result for the trace distance:

$$\min_{\sigma \in \mathcal{S}(A:B)} \|\phi - \sigma\|_1 \geq 2\big(1 - 2^{-2n}\big). \tag{3.2}$$

In fact, a much stronger statement holds: every maximally entangled state is exponentially far from separable not only in trace distance, but also in one-way LOCC distance. It appears that this observation has not yet been made explicitly in the literature, though it is implied by prior results on entanglement purification protocols [10, 7, 3, 43]. We provide a new proof.

Theorem 3.1 (Minimum one-way LOCC distance to separable)**.** *For all maximally entangled pure states $|\phi\rangle$ of two n-qubit registers AB it holds that*

$$\min_{\sigma \in \mathcal{S}(A:B)} \|\phi - \sigma\|_{\text{1-LOCC}} \geq 2(1 - (2/3)^n). \tag{3.3}$$

Moreover, this bound is witnessed by a fixed *one-way LOCC measurement that depends only on $|\phi\rangle$.*

Proof. Let $A^n := A_1 \cdots A_n$ denote Alice's n qubits, and let $B^n := B_1 \cdots B_n$ denote Bob's. By the local unitary equivalence of maximally entangled states, it suffices to exhibit a fixed one-way LOCC measurement that successfully distinguishes any separable state $\sigma_{A^n:B^n}$ from n singlets

$$\bigotimes_{i=1}^{n} |\psi^-\rangle_{A_i B_i}, \tag{3.4}$$

each in the state $|\psi^-\rangle := (|01\rangle - |10\rangle)/\sqrt{2}$. One such scheme is as follows:

1. (Twirling) Bob selects n 2×2 unitaries $\{U_1, \ldots, U_n\}$ at random according to the Haar measure and applies unitary U_i to his ith qubit. He reports to Alice which unitaries he selected and she applies U_i to her ith qubit. This "twirling" step has the effect of symmetrizing their state so that it is a mixture of Bell states.

2. For $i \in \{1, \ldots, n\}$, Bob picks one of the following three Pauli operators

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y = iXZ \tag{3.5}$$

   at random. Let P_i denote the ith choice. He measures P_i on his ith qubit. After performing the last measurement, he sends all measurement choices and outcomes to Alice.

3. For $i \in \{1,\ldots,n\}$, Alice measures P_i on her ith qubit.

4. She accepts that the state is n singlets if and only if all measurement outcomes are different.

The main reason that this 1-LOCC distinguishing protocol works is as follows: the singlet is the only state having the property that measurement outcomes are different when performing the same von Neumann measurement on each qubit (for any von Neumann measurement). Furthermore, the maximum probability with which a separable state can pass this test is equal to 2/3, so that performing n of these tests on a separable state $\sigma_{A^n:B^n}$ reduces the probability of passing the "singlet test" to $(2/3)^n$.

We now analyze this protocol in more detail. Due to the fact that $(U \otimes U)|\psi^-\rangle = |\psi^-\rangle$ for any 2×2 unitary U, the first step has no effect on the singlets. Furthermore, the rest of the protocol succeeds with probability one if the state is equal to n singlets, due to the property mentioned in the previous paragraph. So we turn to analyzing the probability of accepting if the state is in fact separable. We begin by analyzing the first "Pauli test" in steps 2-4 and find a bound on its acceptance probability. When doing so, it suffices to consider the reduced state of $\sigma_{A^n:B^n}$ on systems A_1 and B_1, which is separable across this cut because the original state is separable across the $A^n : B^n$ cut. The initial twirling procedure transforms this separable state to the following "Werner" state:

$$p|\psi^-\rangle\langle\psi^-|_{A_1B_1} + \frac{1-p}{3}\Big(|\psi^+\rangle\langle\psi^+|_{A_1B_1} + |\phi^+\rangle\langle\phi^+|_{A_1B_1} + |\phi^-\rangle\langle\phi^-|_{A_1B_1}\Big), \tag{3.6}$$

such that the maximal value of p is $1/2$ [49, Section VI-B-9]. (The states $|\psi^+\rangle_{A_1B_1}$, $|\phi^+\rangle_{A_1B_1}$, and $|\phi^-\rangle_{A_1B_1}$ are the other Bell states orthogonal to $|\psi^-\rangle_{A_1B_1}$.) One can check that the probability with which each of the three other Bell states besides $|\psi^-\rangle_{A_1B_1}$ passes the "Pauli test" on the ith qubit (in steps 2-4 above) is equal to 1/3. So this implies that the maximum probability with which this Pauli test can pass is $1/2\cdot 1 + 1/6\cdot(1/3+1/3+1/3) = 2/3$. The analysis is the same for the other $n-1$ Pauli tests: the only property that we use is that the reduced states on systems $A_i : B_i$ is separable across this cut, so that entanglement (or any correlation whatsoever) in the systems $A_1\cdots A_n$ or $B_1\cdots B_n$ (but not across the cut $A^n : B^n$) cannot help in passing this test. This property follows from the facts that (i) the initial state is separable across the $A^n : B^n$ cut, (ii) the scheme is LOCC with respect to this cut, and (iii) separability is preserved under LOCC. The result is that $(2/3)^n$ is a universal bound on the maximum probability with which any separable state $\sigma_{A^n:B^n}$ can pass the overall test. By the discussion in Sections 2.2 and 2.4, the statement in the theorem follows. □

4 PURE PRODUCT STATE is BQP-complete

We begin with the simplest of our separability testing promise problems—that of determining whether the state prepared by a given quantum circuit is close to a pure product state. We propose two variants of this problem, one easier than the other. We prove that the harder variant is in BQP and we prove that the easier variant is BQP-hard, establishing BQP-completeness for both problems.

Problem 4.1 ((α,β,ℓ)-PURE PRODUCT STATE[3]).

[3] If $\ell = 2$ then the problem is called (α,β)-BIPARTITE PURE PRODUCT STATE. This convention applies to other problem names throughout the paper.

Input: A description of a quantum circuit that prepares an ℓ-partite pure state $|\psi\rangle$.

Yes: $|\psi\rangle$ is α-close to a pure product state:

$$\min_{|\phi_1\rangle,\dots,|\phi_\ell\rangle} \|\psi - \phi_1 \otimes \cdots \otimes \phi_\ell\|_1 \leq \alpha\,. \tag{4.1}$$

No: $|\psi\rangle$ is β-far from any pure product state:

$$\min_{|\phi_1\rangle,\dots,|\phi_\ell\rangle} \|\psi - \phi_1 \otimes \cdots \otimes \phi_\ell\|_1 \geq \beta\,. \tag{4.2}$$

We define the *one-way LOCC version* of (α,β,ℓ)-PURE PRODUCT STATE similarly except that the trace norm in the specification of a no-instance is replaced with the one-way LOCC norm. The one-way LOCC version of PURE PRODUCT STATE trivially reduces to the trace distance version by virtue of the inequality $\|X\|_1 \geq \|X\|_{\text{1-LOCC}}$. The main result of this section is the following theorem:

Theorem 4.2 (PURE PRODUCT STATE is BQP-complete)**.** *The following hold:*

1. *The trace distance version of* (α,β,ℓ)-PURE PRODUCT STATE[4] *is in* BQP *for all* ℓ *and* $\alpha < \beta\frac{\sqrt{11}}{32}$.
2. *The one-way LOCC version of* $(\varepsilon, 2-\varepsilon)$-BIPARTITE PURE PRODUCT STATE *is* BQP*-hard, even when* ε *decays exponentially in the input length.*

Thus, both problems are BQP*-complete for all* $\ell \geq 2$ *and all* (α,β) *with* $0 < \alpha < \beta\frac{\sqrt{11}}{32}$ *and* $\beta < 2$.

4.1 Membership in BQP

Our efficient quantum algorithm for the PURE PRODUCT STATE problem employs the *product test*. The product test is a boolean test that takes as input two copies of an arbitrary multipartite pure state $|\psi\rangle$. The closer $|\psi\rangle$ is to a product state, the higher the probability with which the product test passes. A specification of the product test is as follows:

1. Given are two copies of an arbitrary ℓ-partite pure state $|\psi\rangle$. One of these copies is contained in registers $A_1,\dots,A_\ell$ and the other in $B_1,\dots,B_\ell$.
2. Perform ℓ swap tests—one for each pair of registers (A_i,B_i) for $i = 1,\dots,\ell$. Accept if and only if all the swap tests pass.

The relationship between the distance from $|\psi\rangle$ to the nearest product state and the success probability of the product test was established in [44].

Theorem 4.3 ([44])**.** *For each ℓ-partite pure state $|\psi\rangle$ let $P_{\text{test}}(\psi)$ denote the probability with which the product test passes when applied to $|\psi\rangle$ and let*

$$1-\varepsilon = \max_{|\phi_1\rangle,\dots,|\phi_\ell\rangle} |\langle\psi|\phi_1 \otimes \cdots \otimes \phi_\ell\rangle|^2. \tag{4.3}$$

[4] It is implicit here and throughout the rest of the paper that the gap between α and $\beta\frac{\sqrt{11}}{32}$ is larger than an inverse polynomial in the input length.

It holds that

$$1-2\varepsilon \le P_{\text{test}}(\psi) \le 1-\frac{11}{512}\varepsilon\,. \tag{4.4}$$

The bounds of Theorem 4.3 are easily written in terms of the trace distance t between $|\psi\rangle$ and the nearest product state via (2.5):

$$1-t^2/2 \le P_{\text{test}}(\psi) \le 1-\frac{11}{2048}t^2. \tag{4.5}$$

Armed with the product test, we now present our quantum algorithm for the PURE PRODUCT STATE problem.

Proposition 4.4. (α,β,ℓ)-PURE PRODUCT STATE *is in* BQP *for all* ℓ *and all* $\alpha < \beta\frac{\sqrt{11}}{32}$.

Proof. The efficient quantum algorithm for (α,β,ℓ)-PURE PRODUCT STATE is as follows: use the input circuit to prepare two copies of $|\psi\rangle$, perform the product test, and accept if and only if the product test passes.

If $|\psi\rangle$ is a yes-instance then (4.5) tells us that the product test passes with probability at least $1-\alpha^2/2$. On the other hand, if $|\psi\rangle$ is a no-instance then (4.5) tells us that the product test passes with probability at most $1-(11/2048)\beta^2$. The algorithm witnesses membership in BQP whenever the former quantity is larger than the latter, which occurs whenever $\alpha < \beta\cdot\sqrt{11}/32$. □

4.2 Hardness for BQP

Proposition 4.5. *The one-way LOCC version of* $(\varepsilon, 2-\varepsilon)$-BIPARTITE PURE PRODUCT STATE *is* BQP-*hard, even when* ε *decays exponentially in the input length.*

Proof. Let L be any promise problem in BQP and let $\{|\nu\rangle_x\}_x$ be a family of efficiently preparable pure states witnessing membership of L in BQP. By this we mean the following: for each instance x of L the state $|\nu_x\rangle$ is held in two registers DG. Register D is a decision qubit indicating acceptance or rejection of x and register G is a garbage register that is a purifying system for D.

Suppose that the family $\{|\nu\rangle_x\}_x$ has completeness $1-\delta$ and soundness δ. In this proof we reduce the arbitrary problem L to the one-way LOCC version of (α,β)-BIPARTITE PURE PRODUCT STATE where

$$\alpha = 2\sqrt{\delta}\,, \tag{4.6}$$

$$\beta = 2-2^{2-n/2}-2\sqrt{\delta}\,, \tag{4.7}$$

for any desired n. The desired hardness result then follows by an appropriate choice of δ, n, given that $\mathsf{BQP}(c,s) \subseteq \mathsf{BQP}(\delta, 1-\delta)$ for any δ exponentially small in the input length.

The reduction is as follows. Given an instance x of L we produce a description of the following circuit for preparing a pure state $|\psi\rangle$ of registers $AA'BDG$:

1. Prepare registers AA' in a $2n$-qubit maximally entangled state such as n EPR pairs, which we denote by $|\phi^+\rangle$. Prepare register B in the n-qubit $|0\rangle$ state. Prepare registers DG in state $|\nu_x\rangle$.

2. Perform a controlled swap gate that swaps registers A' and B when D is in the reject state $|\text{no}\rangle$ and acts as the identity otherwise.

A graphical depiction of this state preparation circuit appears later in the paper as a special case of Figure 3.

If x is a yes-instance of L then $|\nu_x\rangle$ has squared overlap at least $1-\delta$ with $|\text{yes}\rangle_D|\zeta\rangle_G$ for some state $|\zeta\rangle$ of register G. It follows that the constructed state $|\psi\rangle$ is $2\sqrt{\delta}$-close in trace distance to $|\phi^+\rangle_{AA'}|0\rangle_B|\text{yes}\rangle_D|\zeta\rangle_G$, which is a product with respect to the cut $AA' : BDG$. So $|\psi\rangle$ is a yes-instance of the one-way LOCC version of (α,β)-BIPARTITE PURE PRODUCT STATE.

Next, suppose that x is a no-instance of L. In this case $|\nu_x\rangle$ has squared overlap at least $1-\delta$ with $|\text{no}\rangle_D|\eta\rangle_G$ for some state $|\eta\rangle$ of register G. It follows that $|\psi\rangle$ is $2\sqrt{\delta}$-close in trace distance to a state which is in tensor product with the $2n$-qubit maximally entangled state $|\phi^+\rangle$ on registers AB. By contrast, for any product state $|\phi\rangle$ of registers $AA' : BDG$ the reduced state $\operatorname{Tr}_{A'DG}(\phi)$ of registers AB must also be a product state. Thus, it suffices to exhibit a fixed one-way LOCC measurement that successfully distinguishes any product state of registers AB from n EPR pairs with high probability. The existence of such a measurement was proved in Theorem 3.1.

We therefore have the following for any product state $|\phi\rangle$ of registers $AA' : BDG$:

$$\begin{aligned}\|\psi-\phi\|_{\text{1-LOCC}} &\geq \left\|\operatorname{Tr}_{A'DG}(\phi)-\phi^+_{AB}\right\|_{\text{1-LOCC}} - \left\|\phi^+_{AB}-\operatorname{Tr}_{A'DG}(\psi)\right\|_{\text{1-LOCC}} && (4.8)\\ &\geq 2-2^{2-n/2}-2\sqrt{\delta}\,, && (4.9)\end{aligned}$$

from which it follows that $|\psi\rangle$ is a no-instance of the one-way LOCC version of (α,β)-BIPARTITE PURE PRODUCT STATE. □

5 SEPARABLE ISOMETRY OUTPUT (one-way LOCC version) is QMA-complete

In this section we prove QMA-completeness of the problem of deciding whether the isometry implemented by a given quantum circuit can be made to produce a state that is close to separable in trace distance or far from separable in one-way LOCC distance.

Problem 5.1 ((α,β,ℓ)-SEPARABLE ISOMETRY OUTPUT, one-way LOCC version)**.**

Input: A description of a quantum circuit that implements an isometry U with an ℓ-partite output system $A_1\cdots A_\ell$.

Yes: There is an input state ρ such that $U\rho U^*$ is α-close in trace distance to separable:

$$\min_{\rho}\min_{\sigma\in\mathcal{S}(A_1:\cdots:A_\ell)}\|U\rho U^*-\sigma\|_1\leq\alpha\,. \tag{5.1}$$

No: For all input states ρ it holds that $U\rho U^*$ is β-far in one-way LOCC distance from separable:

$$\min_{\rho}\min_{\sigma\in\mathcal{S}(A_1:\cdots:A_\ell)}\|U\rho U^*-\sigma\|_{\text{1-LOCC}}\geq\beta. \tag{5.2}$$

The main result of this section is the following theorem:

Theorem 5.2 (SEPARABLE ISOMETRY OUTPUT, one-way LOCC version is QMA-complete)**.** *The following hold:*

1. *The one-way LOCC version of* (α,β,ℓ)-SEPARABLE ISOMETRY OUTPUT *is in* QMA *for all* ℓ *and all* $\alpha < \beta^4/16$.
2. *The one-way LOCC version of* $(\varepsilon, 2-\varepsilon)$-BIPARTITE SEPARABLE ISOMETRY OUTPUT *is* QMA-*hard, even when* ε *decays exponentially in the input length.*

Thus, the problem is QMA-*complete for all* $\ell \geq 2$, *all* $0 < \alpha < \beta^4/16$, *and all* $\beta < 2$.

5.1 Containment in QMA

Our quantum witness for separability invokes the notion of k-extendibility of separable states [76]. We therefore begin with a brief summary of k-extendibility.

Let AB be any two registers and let $B_1,\ldots,B_k$ be registers each of the same size as B. A bipartite state ρ of registers AB is *k-extendible* if there exists a state ω of registers $AB_1\cdots B_k$ that is invariant under permutations of registers $B_1,\ldots,B_k$ and consistent with ρ, meaning that $\mathrm{Tr}_{B_2\cdots B_k}(\omega)=\rho$.

The set of all k-extendible states (with respect to a given cut of the registers) is denoted $\mathcal{E}_k$. It is a basic fact that every separable state is k-extendible for all k, so that $\mathcal{S}\subseteq\mathcal{E}_k$. To see this, let

$$\rho=\sum_i p_i|\psi^i\rangle\langle\psi^i|_A\otimes|\phi^i\rangle\langle\phi^i|_B \tag{5.3}$$

be any separable state of registers AB and observe that

$$\sum_i p_i|\psi^i\rangle\langle\psi^i|_A\otimes|\phi^i\rangle\langle\phi^i|_B^{\otimes k} \tag{5.4}$$

is a k-extension of ρ. It is known that if ρ is not separable then there exists some k' for which ρ is not k'-extendible. Moreover, it is known that $\mathcal{E}_{k+1}\subseteq\mathcal{E}_k$ for all k, from which it follows that the sets $\mathcal{E}_k$ form a containment hierarchy that converges to the set $\mathcal{S}$ of separable states in the limit $k\to\infty$ [31, 32].

The notion of k-extendibility extends naturally to multi-register systems $A_1\cdots A_\ell$ by imposing the extendibility condition on each individual register [33, 19], though the notation is cumbersome. Formally, let $A_{i,1},\ldots,A_{i,k}$ be registers of the same size as A_i. A state ρ of registers $A_1\cdots A_\ell$ is k-extendible with respect to $A_1:\cdots:A_\ell$ if there exists a global state ω of all ℓk registers $A_{i,j}$ that is consistent with ρ on $A_1\cdots A_\ell$ and invariant under permutations of registers $A_{i,1},\ldots,A_{i,k}$ for all $i=1,\ldots,\ell$. (Observe that there are $\ell\cdot k!$ such permutations.)

Brandão and Harrow have shown that if ρ is close to k-extendible in trace distance for not-too-large k then ρ is also close to separable in one-way LOCC distance [19]. The following is a straightforward consequence of their result.

Theorem 5.3. *Let* $A_1,\ldots,A_\ell$ *be registers whose total combined dimension is* D. *Let* ρ *be* ε-*far from separable in one-way LOCC distance, so that*

$$\min_{\sigma\in\mathcal{S}(A_1:\cdots:A_\ell)}\|\rho-\sigma\|_{1\text{-LOCC}}\geq\varepsilon. \tag{5.5}$$

Then for any $\delta < \varepsilon$ it holds that ρ is δ-far from k-extendible in trace distance, so that

$$\min_{\sigma' \in \mathcal{E}_k(A_1:\cdots:A_\ell)} \|\rho - \sigma'\|_1 \geq \delta, \tag{5.6}$$

provided

$$k \geq \left\lceil \ell + \frac{4\ell^2 \log D}{(\varepsilon - \delta)^2} \right\rceil . \tag{5.7}$$

Proof. Let σ' be any k-extendible state with $k > \ell$. We know from [19, Theorem 2 and Corollary 8] that there is a separable state $\sigma'' \in \mathcal{S}$ such that

$$\left\| \sigma' - \sigma'' \right\|_{\text{1-LOCC}} \leq \sqrt{\frac{4\ell^2 \log D}{k - \ell}}. \tag{5.8}$$

So we use this in the following chain of inequalities:

$$\begin{aligned} \varepsilon &\leq \min_{\sigma \in \mathcal{S}(A_1:\cdots:A_\ell)} \|\rho - \sigma\|_{\text{1-LOCC}} && (5.9) \\ &\leq \|\rho - \sigma''\|_{\text{1-LOCC}} && (5.10) \\ &\leq \|\rho - \sigma'\|_{\text{1-LOCC}} + \|\sigma' - \sigma''\|_{\text{1-LOCC}} && (5.11) \\ &\leq \|\rho - \sigma'\|_1 + \sqrt{\frac{4\ell^2 \log D}{k - \ell}} . && (5.12) \end{aligned}$$

Since this bound holds for any k-extendible state, we can conclude that

$$\varepsilon - \sqrt{\frac{4\ell^2 \log D}{k - \ell}} \leq \min_{\sigma' \in \mathcal{E}_k(A_1:\cdots:A_\ell)} \|\rho - \sigma'\|_1 . \tag{5.13}$$

The statement of the theorem then follows by picking k large enough so that

$$\varepsilon - \sqrt{\frac{4\ell^2 \log D}{k - \ell}} \geq \delta . \qquad \square$$

We now present our succinct quantum witness for the one-way LOCC version of the SEPARABLE ISOMETRY OUTPUT problem.

Proposition 5.4. *The one-way LOCC version of (α, β, ℓ)-SEPARABLE ISOMETRY OUTPUT is in* QMA *for all ℓ and all $\alpha < \beta^4/16$.*

Proof. For convenience we write $A := A_1 \cdots A_\ell$ where the combined register A has dimension D. It is helpful to label the input and output registers of U as $U : S \to A$. Let $\varepsilon > 0$ be such that $\sqrt{\alpha} < (\beta - \varepsilon)^2/4$. The verifier witnessing membership of the problem in QMA is as follows:

1. Receive $k\ell+1$ registers from the prover labeled S and A_i^j where A_i^j has the same size as A_i for $i=1,\dots,\ell$ and $j=1,\dots,k$ and
$$k=\left\lceil \ell+\frac{4\ell^2\log D}{\varepsilon^2}\right\rceil . \tag{5.14}$$
Apply U to register S to obtain register $A:=A_1,\dots,A_\ell$.

2. Perform ℓ permutation tests: one for each group $(A_i,A_i^1,\dots,A_i^k)$ of $k+1$ registers. Accept if and only if all permutation tests pass.

In what follows we use the shorthand $A^j:=A_1^j\cdots A_\ell^j$ for each $j\in\{1,\dots,k\}$.

Suppose first that U is a yes-instance of the problem. We show that there exists a state $\rho_{SA^1\dots A^k}$ of the $k\ell+1$ registers $SA^1\cdots A^k$ that causes the verifier to accept with probability at least $1-\sqrt{\alpha}$. To this end we define the following symbols:

1. Let σ_A be a separable state and ρ_S be a state of register S such that
$$\|U\rho_S U^*-\sigma_A\|_1\le\alpha\,, \tag{5.15}$$
as promised in (5.1).

2. Let $\sigma_{AA^1\dots A^k}$ be a $(k+1)$-extension of σ_A in registers $AA^1\cdots A^k$. It is important that this $(k+1)$-extension be taken as a convex combination of pure states as in (5.4), so that it would be accepted by the permutation test with probability one.

3. Let $\hat{U}:SW\to A$ denote the unitary circuit that implements U when the workspace register W is initialized to $|0\rangle$.

By the preservation of subsystem fidelity [51, Lemma 7.2] there exists a state $\rho_{SA^1\dots A^k}$ of registers $SA^1\cdots A^k$ consistent with ρ_S such that
$$F\big((\hat{U}^*\otimes I_{A^1\dots A^k})\sigma_{AA^1\dots A^k}(\hat{U}\otimes I_{A^1\dots A^k}),\rho_{SA^1\dots A^k}\otimes|0\rangle\langle 0|_W\big)=F\big(\hat{U}^*\sigma_A\hat{U},\rho_S\otimes|0\rangle\langle 0|_W\big)\,. \tag{5.16}$$

Let us argue that this state $\rho_{SA^1\dots A^k}$ is our desired state. It follows from (2.9), (5.15), and unitary invariance of fidelity that
$$\begin{aligned}1-\alpha&\le F\big(\sigma_A,\hat{U}(\rho_S\otimes|0\rangle\langle 0|_W)\hat{U}^*\big) &(5.17)\\ &=F\big(\hat{U}^*\sigma_A\hat{U},\rho_S\otimes|0\rangle\langle 0|_W\big)\,. &(5.18)\end{aligned}$$

Applying the above and (2.9) to the right side of (5.16), we find that the quantity in (5.16) is at least
$$1-\big\|\hat{U}^*\sigma_A\hat{U}-\rho_S\otimes|0\rangle\langle 0|_W\big\|_1\ge 1-\alpha\,. \tag{5.19}$$

Applying (2.9) to the left side of (5.16), we find that the quantity in (5.16) is at most
$$1-\frac{1}{4}\big\|(\hat{U}^*\otimes I_{A^1\dots A^k})\sigma_{AA^1\dots A^k}(\hat{U}\otimes I_{A^1\dots A^k})-\rho_{SA^1\dots A^k}\otimes|0\rangle\langle 0|_W\big\|_1^2\,. \tag{5.20}$$

Combining (5.19) and (5.20) leads to the following bound:

$$\|\sigma_{AA^1\cdots A^k} - (U \otimes I_{A^1\cdots A^k})\rho_{SA^1\cdots A^k}(U^* \otimes I_{A^1\cdots A^k})\|_1 \leq 2\sqrt{\alpha}\,. \tag{5.21}$$

Thus, $\rho_{SA^1\cdots A^k}$ is $2\sqrt{\alpha}$-close in trace distance to a state that is accepted by the verifier with certainty. It then follows from (2.4) that the verifier accepts $\rho_{SA^1\cdots A^k}$ with probability at least $1-\sqrt{\alpha}$ as desired.

Now suppose that U is a no-instance of the problem. By Theorem 5.3 and our choice of k we have that

$$\min_{\rho_S} \min_{\sigma_A \in \mathcal{E}_k(A_1:\cdots:A_\ell)} \|U\rho_S U^* - \sigma_A\|_1 \geq \beta - \varepsilon\,. \tag{5.22}$$

We claim that an upper bound on the probability with which all the permutation tests pass is given by the maximum fidelity of $U\rho_S U^*$ with a k-extendible state:

$$\Pr[\text{all pass}] \leq \max_{\rho_S} \max_{\sigma_A \in \mathcal{E}_k} F(U\rho_S U^*, \sigma_A)\,. \tag{5.23}$$

It follows from (2.9) that this probability is at most $1-(\beta-\varepsilon)^2/4$. We chose ε so that the completeness $1-\sqrt{\alpha}$ is larger than the soundness $1-(\beta-\varepsilon)^2/4$, from which it follows that the problem is in QMA.

We now justify the claim in (5.23) using a method similar to that in [46, Section 4]. In order to implement the permutation tests in step 2 the verifier prepares a control register C in state

$$|\text{perm}\rangle_C := \frac{1}{\sqrt{k!}} \sum_{\pi \in S_k} |\pi\rangle_C\,, \tag{5.24}$$

which is a uniform superposition over all possible permutations of k elements resulting from an application of the quantum Fourier transform [63] to the state $|0\rangle_C$, so that the C register requires $\lceil \log_2(k!) \rceil$ qubits. The verifier then applies the following controlled-permutation operation:

$$(U_\Pi)_{AA^1\cdots A^k C} := \sum_{\pi \in S_k} W^\pi_{AA^1\cdots A^k} \otimes |\pi\rangle\langle\pi|_C\,, \tag{5.25}$$

where $W^\pi_{AA^1\cdots A^k}$ is a unitary operation corresponding to permutation π. The verifier finally applies an inverse quantum Fourier transform to C, measures it in the computational basis, and accepts if the measurement outcomes are all zeros. Letting $|\psi\rangle_{RSA^1\cdots A^k}$ be a purification of the prover's input, we can write the maximum acceptance probability of this proof system as follows:

$$\begin{aligned}
&\max_{|\psi\rangle_{RSA^1\cdots A^k}} \left\| \langle 0|_C \mathrm{QFT}_C^{-1} (U_\Pi)_{AA^1\cdots A^k C} U_{S\to A} |\psi\rangle_{RSA^1\cdots A^k} |\text{perm}\rangle_C \right\|_2^2 \\
&\quad = \max_{|\psi\rangle_{RSA^1\cdots A^k}, |\phi\rangle_{RAA^1\cdots A^k}} \left| \langle 0|_C \langle\phi|_{RAA^1\cdots A^k} \mathrm{QFT}_C^{-1} (U_\Pi)_{AA^1\cdots A^k C} U_{S\to A} |\psi\rangle_{RSA^1\cdots A^k} |\text{perm}\rangle_C \right|_2^2.
\end{aligned} \tag{5.26}$$

We can define a channel generated by the inverse of the verifier's circuit conditioned on accepting as follows:

$$\mathcal{M}_{AA^1\cdots A^k \to AC}(\sigma_{AA^1\cdots A^k}) := \mathrm{Tr}_{A^1\cdots A^k}\{(U_\Pi)_{AA^1\cdots A^k C}(\sigma_{AA^1\cdots A^k} \otimes |\text{perm}\rangle\langle\text{perm}|_C)(U_\Pi^*)_{AA^1\cdots A^k C}\}\,. \tag{5.27}$$

After doing so, we can apply Uhlmann's theorem to (5.26) to rewrite the maximum acceptance probability as follows:

$$\max_{\rho_S,\sigma_{AA^1\dots A^k}} F\left(U_{S\to A}\rho_S U^*_{S\to A}\otimes|\mathrm{perm}\rangle\langle\mathrm{perm}|_C,\mathcal{M}_{AA^1\dots A^k\to AC}(\sigma_{AA^1\dots A^k})\right). \tag{5.28}$$

Since the fidelity can only increase under the discarding of the control register C,[5] the maximum acceptance probability is upper bounded by the following quantity:

$$\max_{\rho_S,\sigma_{AA^1\dots A^k}} F\left(U_{S\to A}\rho_S U^*_{S\to A},\mathcal{M}_{AA^1\dots A^k\to A}(\sigma_{AA^1\dots A^k})\right), \tag{5.29}$$

where

$$\begin{aligned}\mathcal{M}_{AA^1\dots A^k\to A}(\sigma_{AA^1\dots A^k}) &= \mathrm{Tr}_C\{\mathcal{M}_{AA^1\dots A^k\to AC}(\sigma_{AA^1\dots A^k})\} \\ &= \frac{1}{k!}\sum_{\pi\in S_k}\mathrm{Tr}_{A^1\dots A^k}\left\{W^{\pi}_{AA^1\dots A^k}\sigma_{AA^1\dots A^k}\left(W^{\pi}_{AA^1\dots A^k}\right)^*\right\},\end{aligned} \tag{5.30}$$

The equation above reveals that $\mathcal{M}_{AA^1\dots A^k\to A}$ is just the channel that applies a random permutation of the $AA^1\cdots A^k$ systems and discards the last k systems $A^1\cdots A^k$. Clearly, since the channel $\mathcal{M}_{AA^1\dots A^k\to A}$ symmetrizes the state of the systems $AA^1\cdots A^k$, the maximum in (5.29) is achieved by a state $\sigma_{AA^1\dots A^k}$ for which systems $AA^1\cdots A^k$ are permutation symmetric. Thus, by recalling the definition of k-extendibility, we can rewrite (5.29) as the maximum k-extendible fidelity of $U_{S\to A}\rho_S U^*_{S\to A}$:

$$\max_{\rho_S,\sigma_{AA^1\dots A^k}} F\left(U_{S\to A}\rho_S U^*_{S\to A},\mathcal{M}_{AA^1\dots A^k\to A}(\sigma_{AA^1\dots A^k})\right) = \max_{\rho_S,\sigma_A\in\mathcal{E}_k(A_1:\dots:A_\ell)} F\left(U_{S\to A}\rho_S U^*_{S\to A},\sigma_A\right). \tag{5.31}$$

This demonstrates that the maximum k-extendible fidelity is an upper bound on the maximum acceptance probability and completes our proof of the claim in (5.23). □

5.2 Hardness for QMA

Proposition 5.5. *The one-way LOCC version of* $(\varepsilon,2-\varepsilon)$-BIPARTITE SEPARABLE ISOMETRY OUTPUT *is* QMA-*hard, even when* ε *decays exponentially in the input length.*

Proof. This proof is almost exactly the same as the proof of Proposition 4.5. The only difference is that here we must quantify over all states of a new input register P for each circuit. Nonetheless, we include a full proof for completeness.

Let L be any promise problem in QMA and let $\{V_x\}_x$ be a family of isometric verifier circuits witnessing this fact with completeness $1-\delta$ and soundness δ for sufficiently small δ to be chosen later. Circuits in this family take the form $V_x : P\to DG$. The input register P is supplied by the prover. The output register D is a decision qubit indicating acceptance or rejection of x and the output register G is a garbage register that holds the purification of D.

[5] We can interpret discarding the control register as actually giving it to the prover, so that the resulting fidelity corresponds to the maximum acceptance probability in a modified protocol in which the prover controls the inputs to C.

In this proof we reduce the arbitrary problem L to the one-way LOCC version of (α,β)-BIPARTITE SEPARABLE ISOMETRY OUTPUT where

$$\alpha = 2\sqrt{\delta}\,, \tag{5.32}$$

$$\beta = 2 - 2^{2-n/2} - 2\sqrt{\delta}\,, \tag{5.33}$$

for any desired n. The desired hardness result then follows by an appropriate choice of δ, n.

The reduction is as follows. Given an instance x of L we produce a description of the following isometric circuit $U : P \to AA'BDG$:

1. Given the input register P apply the verifier circuit V_x to obtain registers DG.
2. Prepare registers AA' in a $2n$-qubit maximally entangled state such as n EPR pairs, which we denote by $|\phi^+\rangle$. Prepare register B in the n-qubit $|0\rangle$ state.
3. Perform a unitary conditional swap gate that swaps registers A' and B when D is in the reject state $|\text{no}\rangle$ and acts as the identity otherwise.

See Figure 3 for a graphical depiction of this circuit.

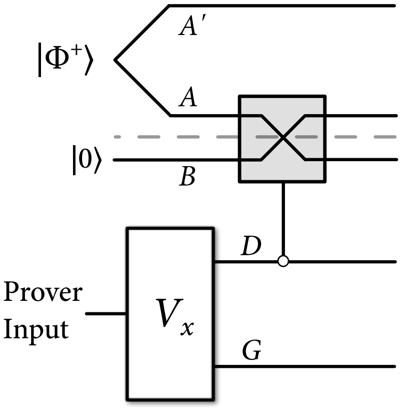


Figure 3: The circuit U produced by our reduction from an arbitrary problem $L \in \mathsf{QMA}$ to the one-way LOCC version of $(\varepsilon, 2-\varepsilon)$-BIPARTITE SEPARABLE ISOMETRY OUTPUT. The dashed line indicates that the output registers are to be divided along the bipartite cut $AA' : BDG$. This construction also appears in the proof of Proposition 4.5 in the special case where the prover's input is empty.

Suppose x is a yes-instance of L and let $|\varpi\rangle$ be a pure state of register P that causes the verifier to accept with high probability, meaning that the state $V_x|\varpi\rangle$ has squared overlap at least $1-\delta$ with $|\text{yes}\rangle_D|\zeta\rangle_G$ for some state $|\zeta\rangle$ of register G. It follows that $U|\varpi\rangle$ is $2\sqrt{\delta}$-close in trace distance to $|\phi^+\rangle_{AA'}|0\rangle_B|\text{yes}\rangle_D|\zeta\rangle_G$, which is a product with respect to the cut $AA' : BDG$, and so U is a yes-instance of the one-way LOCC version of (α,β)-BIPARTITE SEPARABLE ISOMETRY OUTPUT.

Next, suppose that x is a no-instance of L. In this case for all input states ρ of register P the output state $U\rho U^*$ of registers $AA'BDG$ is $2\sqrt{\delta}$-close to a state which is in tensor product with the $2n$-qubit maximally entangled state $|\phi^+\rangle$ on registers AB. By contrast, for any separable state σ of registers $AA' : BDG$ the reduced state $\mathrm{Tr}_{A'DG}(\sigma)$ of registers AB must also be separable. Thus, it suffices to exhibit a fixed one-way LOCC measurement that successfully distinguishes any separable state of registers AB from n EPR pairs with high probability. The existence of such a measurement was proved in Theorem 3.1.

We therefore have the following for any input state ρ of register P and any separable state σ of registers $AA' : BDG$:

$$\|U\rho U^* - \sigma\|_{\text{1-LOCC}} \geq \left\|\mathrm{Tr}_{A'DG}(\sigma) - \phi^+_{AB}\right\|_{\text{1-LOCC}} - \left\|\phi^+_{AB} - \mathrm{Tr}_{A'DG}(U\rho U^*)\right\|_{\text{1-LOCC}} \tag{5.34}$$

$$\geq 2 - 2^{2-n/2} - 2\sqrt{\delta}\,, \tag{5.35}$$

from which it follows that U is a no-instance of the one-way LOCC version of (α,β)-BIPARTITE SEPARABLE ISOMETRY OUTPUT. □

6 SEPARABLE ISOMETRY OUTPUT is QMA(2)-complete

In Section 5 we showed that the one-way LOCC version of the SEPARABLE ISOMETRY OUTPUT problem is QMA-complete. By contrast, in this section we show that the trace distance version of this problem (and some closely related variants of it) are QMA(2)-complete.

We begin by restricting attention to the problem of determining whether an isometry U described by a quantum circuit can be made to produce a pure product output state from a pure input state.

Problem 6.1 ((α,β,ℓ)-PURE PRODUCT ISOMETRY OUTPUT)**.**

Input: A description of a quantum circuit that implements an isometry U with an ℓ-partite output system $A_1 \cdots A_\ell$.

Yes: There is an input state $|\psi\rangle$ such that $U|\psi\rangle$ is α-close to a pure product state:

$$\min_{|\psi\rangle} \min_{|\phi_1\rangle,\ldots,|\phi_\ell\rangle} \|U\psi U^* - \phi_1 \otimes \cdots \otimes \phi_\ell\|_1 \leq \alpha\,. \tag{6.1}$$

No: For all input states $|\psi\rangle$ it holds that $U|\psi\rangle$ is β-far from a pure product state:

$$\min_{|\psi\rangle} \min_{|\phi_1\rangle,\ldots,|\phi_\ell\rangle} \|U\psi U^* - \phi_1 \otimes \cdots \otimes \phi_\ell\|_1 \geq \beta\,. \tag{6.2}$$

The main result of this section is the following theorem:

Theorem 6.2 (PURE PRODUCT ISOMETRY OUTPUT is QMA(2)-complete)**.** *The following hold:*

1. (α,β,ℓ)-PURE PRODUCT ISOMETRY OUTPUT *is in* QMA(2) *for all* ℓ *and all* $\alpha < \beta$.
2. $(\varepsilon, 2-\varepsilon)$-BIPARTITE PURE PRODUCT ISOMETRY OUTPUT *is* QMA(2)*-hard, even when* ε *decays exponentially in the input length.*

Thus, the problem is QMA(2)*-complete for all* $\ell \geq 2$ *and all* $0 < \alpha < \beta < 2$.

6.1 Containment in $\mathsf{QMA}(2)$

Proposition 6.3. (α,β,ℓ)-PURE PRODUCT ISOMETRY OUTPUT *is in* $\mathsf{QMA}(2)$ *for all* ℓ *and all* $\alpha < \beta$.

Proof. We prove that the problem is in $\mathsf{QMA}(\ell+1)$, from which it follows that the problem is also in $\mathsf{QMA}(2)$ via the main result of [44]. The verifier witnessing membership of the problem in $\mathsf{QMA}(\ell+1)$ is as follows:

1. Receive an input state $|\psi\rangle$ from one of the provers and a candidate product state $|\phi_1\rangle \otimes \cdots \otimes |\phi_\ell\rangle$ from the remaining ℓ provers.

2. Apply U to the input. Perform a swap test between $U|\psi\rangle$ and $|\phi_1\rangle \otimes \cdots \otimes |\phi_\ell\rangle$. Accept if and only if the swap test passes.

If U is a yes-instance then the provers can cause the verifier to accept with probability at least $1-\alpha^2/8$ by an appropriate choice of states $|\psi\rangle, |\phi_1\rangle, \ldots, |\phi_\ell\rangle$. It follows from a standard convexity argument that the provers achieve their maximum probability of success for the swap test when they each send the verifier a pure state, so we assume that they do so without loss of generality. So if U is a no-instance then the verifier will accept with probability at most $1-\beta^2/8$ regardless of which states the provers send to the verifier. As $\alpha < \beta$, there is a gap between completeness and soundness for this verifier. □

6.2 Hardness for $\mathsf{QMA}(2)$

Proposition 6.4. $(\varepsilon, 2-\varepsilon)$-BIPARTITE PURE PRODUCT ISOMETRY OUTPUT *is* $\mathsf{QMA}(2)$*-hard, even when* ε *decays exponentially in the input length.*

Proof. Let L be any promise problem in $\mathsf{QMA}(2)$ and let $\{V_x\}_x$ be a family of unitary verifier circuits (indexed by instances x of L) witnessing this fact with completeness $1-\delta$ and soundness δ for sufficiently small δ to be chosen later. Circuits in this family take the form $V_x : ABW \to DG$. Such a verifier circuit V_x is depicted in Figure 4(a). The input registers A, B are supplied by the two provers and the input register W is a workspace register initialized to the $|0\rangle$ state. The output register D is a decision qubit indicating acceptance or rejection of x and the output register G is a garbage register that consists of the remaining qubits upon which V_x acts.

In this proof we reduce the arbitrary problem L to (α,β)-BIPARTITE PURE PRODUCT ISOMETRY OUTPUT where

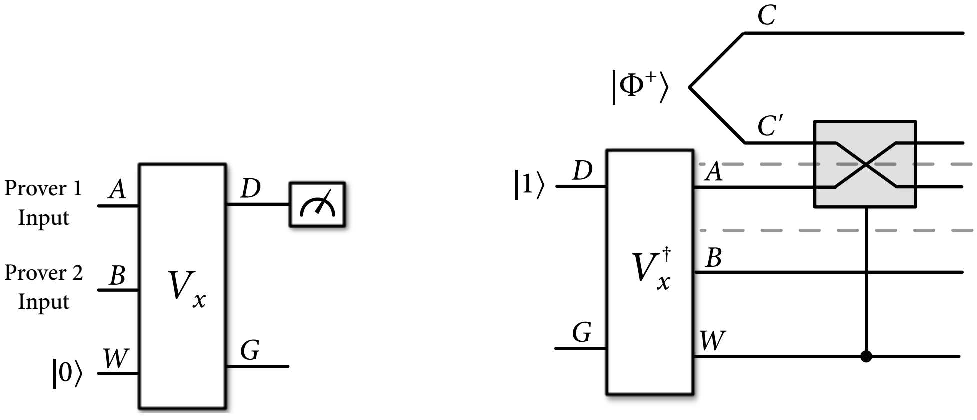
$$\alpha = 2\sqrt{\delta}, \tag{6.3}$$

$$\beta = 2\sqrt{1-\left(\sqrt{\delta}+2^{-n/2}\right)^2}, \tag{6.4}$$

for any desired n. The desired hardness result then follows by an appropriate choice of δ, n.

The reduction is as follows. Given an instance x of L we produce a description of the following isometric circuit $U : G \to ABCC'W$:

1. Given the input register G, prepare a qubit D in the accept state $|\text{yes}\rangle$ and apply the inverse circuit V_x^* to obtain registers ABW.



(a) A QMA(2) verifier.

(b) The circuit produced by our reduction.

Figure 4: (a) A unitary verifier circuit V_x for an arbitrary verifier witnessing membership of L in QMA(2) on input x. (b) The circuit U produced by our reduction. Dashed lines indicate that the output registers are to be divided along the bipartite cut $A : BCC'W$.

2. Prepare registers CC' in a $2n$-qubit maximally entangled state such as n EPR pairs, which we denote by $|\phi^+\rangle$.

3. Perform a unitary conditional swap gate that swaps registers A and C when W is orthogonal to the $|0\rangle$ state and acts as the identity otherwise. (Here we implicitly pad the register A with $|0\rangle$ qubits so as to have the same size as C.)

See Figure 4(b) for a graphical depiction of this circuit.

Let us argue that this construction has the claimed properties. Suppose first that x is a yes-instance of L and let $|\phi\rangle_A|\varphi\rangle_B$ be a pure product state of registers AB that causes the verifier to accept with high probability. That is, the state $V_x|\phi\rangle_A|\varphi\rangle_B|0\rangle_W$ has squared overlap at least $1-\delta$ with $|\text{yes}\rangle|\psi\rangle$ for some state $|\psi\rangle$ of register G. Thus $U|\psi\rangle$ is $2\sqrt{\delta}$-close in trace distance to $|\phi\rangle_A|\varphi\rangle_B|\phi^+\rangle_{CC'}|0\rangle_W$, which is a product with respect to the cut $A : BCC'W$, and so U is a yes-instance of (α,β)-BIPARTITE PURE PRODUCT ISOMETRY OUTPUT.

Next, suppose that x is a no-instance of L. Fix any pure input state $|\psi\rangle$ for register G and observe that

$$U|\psi\rangle = \Pi_0 U|\psi\rangle + (I-\Pi_0)U|\psi\rangle \tag{6.5}$$

where $\Pi_0 = |0\rangle\langle 0|_W$ denotes the projection onto the $|0\rangle$ state for register W. From the definition of the circuit U it is clear that we may write

$$\begin{aligned}
\Pi_0 U|\psi\rangle &= \Pi_0(V_x^*|\text{yes}\rangle|\psi\rangle)\otimes|\phi^+\rangle_{CC'} &(6.6)\\
&= |\zeta_{AB}\rangle|0\rangle_W|\phi^+\rangle_{CC'} &(6.7)\\
(I-\Pi_0)U|\psi\rangle &= \text{Swap}_{AC'}\big((I-\Pi_0)(V_x^*|\text{yes}\rangle|\psi\rangle)\otimes|\phi^+\rangle_{CC'}\big) &(6.8)\\
&= |\xi_{BC'W}\rangle|\phi^+\rangle_{AC} &(6.9)
\end{aligned}$$

for some choice of subnormalized pure states $|\zeta_{AB}\rangle$ and $|\xi_{BC'W}\rangle$ of registers AB and $BC'W$, respectively.

Then for any pure product state $|\phi\rangle$ of registers $A : BCC'W$ it holds that

$$|\langle\phi|U|\psi\rangle| \leq \max_{|\phi'\rangle}\big|\langle\phi'|\Pi_0 U|\psi\rangle\big| + \max_{|\phi''\rangle}\big|\langle\phi''|(I-\Pi_0)U|\psi\rangle\big| \tag{6.10}$$

where the maxima on the right side are also over product states $|\phi'\rangle, |\phi''\rangle$ of registers $A : BCC'W$.

First, let us bound the maximum over $|\phi'\rangle$. It is clear from (6.7) that this maximum is achieved by some $|\phi'\rangle$ of the form

$$|\phi'\rangle = |\phi\rangle_A|\varphi\rangle_B|0\rangle_W|\phi^+\rangle_{CC'}, \tag{6.11}$$

in which case we have

$$\big|\langle\phi'|\Pi_0 U|\psi\rangle\big| = |\langle\phi|_A\langle\varphi|_B\langle 0|_W V_x^*|\text{yes}\rangle|\psi\rangle| \leq \sqrt{\delta} \tag{6.12}$$

where the inequality follows from the assumption that x is a no-instance of L.

Next, let us bound the maximum over $|\phi''\rangle$. Since $(I-\Pi_0)U|\psi\rangle$ is maximally entangled on registers AC, its squared inner product with any product state $|\phi''\rangle$ is at most 2^{-n} as observed in (3.1) of Section 3.

We have thus shown that

$$\max_{|\psi\rangle}\max_{\text{product }|\phi\rangle}|\langle\phi|U|\psi\rangle|^2 \leq \left(\sqrt{\delta}+2^{-n/2}\right)^2 \tag{6.13}$$

and consequently

$$\min_{|\psi\rangle}\min_{\text{product }|\phi\rangle}\|U\psi U^* - \phi\|_1 \geq 2\sqrt{1-\left(\sqrt{\delta}+2^{-n/2}\right)^2}. \tag{6.14}$$

We have thus shown that U is a no-instance of (α,β)-BIPARTITE PURE PRODUCT ISOMETRY OUTPUT. □

6.3 Equivalence of separability testing problems

We also consider two variants of PURE PRODUCT ISOMETRY OUTPUT (Problem 6.1) in which the task is to determine whether an isometry U can be made to produce a (not necessarily pure) product state or a separable state. Whereas Problem 6.1 restricts attention only to pure input states, in the following variants of the problem we also allow arbitrary mixed state inputs. Formal specifications of these two variants of Problem 6.1 are given below.

Problem 6.5 ((α,β,ℓ)-PRODUCT ISOMETRY OUTPUT)**.**

Input: A description of a quantum circuit that implements an isometry U with an ℓ-partite output system $A_1\cdots A_\ell$.

Yes: There is an input state ρ such that $U\rho U^*$ is α-close to a product state:

$$\min_{\rho}\min_{\sigma_1,\ldots,\sigma_\ell}\|U\rho U^* - \sigma_1\otimes\cdots\otimes\sigma_\ell\|_1 \leq \alpha. \tag{6.15}$$

No: For all input states ρ it holds that $U\rho U^*$ is β-far from a product state:

$$\min_{\rho}\min_{\sigma_1,\ldots,\sigma_\ell}\|U\rho U^* - \sigma_1\otimes\cdots\otimes\sigma_\ell\|_1 \geq \beta. \tag{6.16}$$

Problem 6.6 ((α,β,ℓ)-SEPARABLE ISOMETRY OUTPUT)**.**

Input: A description of a quantum circuit that implements an isometry U with an ℓ-partite output system $A_1 \cdots A_\ell$.

Yes: There is an input state ρ such that $U\rho U^*$ is α-close to a separable state:

$$\min_{\rho} \min_{\sigma\in\mathcal{S}(A_1:\cdots:A_\ell)} \|U\rho U^* - \sigma\|_1 \le \alpha\,. \tag{6.17}$$

No: For all input states ρ it holds that $U\rho U^*$ is β-far from separable:

$$\min_{\rho} \min_{\sigma\in\mathcal{S}(A_1:\cdots:A_\ell)} \|U\rho U^* - \sigma\|_1 \ge \beta. \tag{6.18}$$

We now argue that, for each ℓ, these problems are equivalent to one another for a wide range of choices of (α,β). These equivalences are corollaries of the following proposition, which relates minimal distance from separable to minimal distance from pure product.

Proposition 6.7 (Separable-to-pure product reduction)**.** *Let U be an isometry with an ℓ-partite output system $A_1\cdots A_\ell$ and suppose that there is an input state ρ such that $U\rho U^*$ is δ-close to some separable state $\sigma \in \mathcal{S}(A_1 : \cdots : A_\ell)$:*

$$\|U\rho U^* - \sigma\|_1 \le \delta. \tag{6.19}$$

Then there is a pure input state $|\psi\rangle$ such that $U\psi U^*$ is $4\sqrt{\delta}$-close to some pure product state $|\phi_1\rangle \otimes \cdots \otimes |\phi_\ell\rangle$:

$$\|U\psi U^* - \phi_1 \otimes \cdots \otimes \phi_\ell\|_1 \le 4\sqrt{\delta}. \tag{6.20}$$

Proof. Let

$$\sigma = \sum_x p_x \phi_1^x \otimes \cdots \otimes \phi_\ell^x \tag{6.21}$$

be a decomposition of σ as a probabilistic mixture of pure product states and let

$$|\zeta\rangle = \sum_x \sqrt{p_x} |x\rangle_R \otimes |\phi_1^x\rangle \otimes \cdots \otimes |\phi_\ell^x\rangle \tag{6.22}$$

be a purification of σ on registers $RA_1\cdots A_\ell$.

Let S denote the input register for U. It follows from (2.9) and Uhlmann's Theorem that there is a purification $|\psi\rangle$ of ρ on registers RS with

$$\|U\psi U^* - \zeta\|_1 \le 2\sqrt{\delta}. \tag{6.23}$$

Write $|\psi\rangle$ as

$$|\psi\rangle = \sum_x \sqrt{q_x} |x\rangle_R \otimes |\psi^x\rangle \tag{6.24}$$

for some probability vector q and states $\{|\psi^x\rangle\}_x$ (not necessarily orthogonal). Apply a dephasing channel in the basis $\{|x\rangle\}_x$ on register R and use contractivity of trace norm under quantum channels to obtain

$$\|U\psi U^* - \zeta\|_1 \ge \left\| \sum_x q_x |x\rangle\langle x| \otimes U\psi^x U^* - \sum_x p_x |x\rangle\langle x| \otimes \phi_1^x \otimes \cdots \otimes \phi_\ell^x \right\|_1 . \tag{6.25}$$

Combining this bound with the triangle inequality, we have

$$\begin{aligned}
&\sum_x p_x \| U\psi^x U^* - \phi_1^x \otimes \cdots \otimes \phi_\ell^x \|_1 && (6.26)\\
&= \left\| \sum_x p_x |x\rangle\langle x| \otimes (U\psi^x U^* - \phi_1^x \otimes \cdots \otimes \phi_\ell^x) \right\|_1 && (6.27)\\
&\le \left\| \sum_x q_x |x\rangle\langle x| \otimes U\psi^x U^* - \sum_x p_x |x\rangle\langle x| \otimes U\psi^x U^* \right\|_1 && (6.28)\\
&\quad + \left\| \sum_x q_x |x\rangle\langle x| \otimes U\psi^x U^* - \sum_x p_x |x\rangle\langle x| \otimes \phi_1^x \otimes \cdots \otimes \phi_\ell^x \right\|_1 && (6.29)\\
&\le 4\sqrt{\delta}. && (6.30)
\end{aligned}$$

Since this inequality holds for a convex combination over terms indexed by x, it must also hold for at least one choice of $\psi^x, \phi_1^x, \dots, \phi_\ell^x$. □

Corollary 6.8 (Equivalence of problems). *The following hold for all ℓ and all $\alpha < \beta$:*

1. *Both (α,β,ℓ)-PRODUCT ISOMETRY OUTPUT and (α,β,ℓ)-SEPARABLE ISOMETRY OUTPUT trivially reduce to $(4\sqrt{\alpha},\beta,\ell)$-PURE PRODUCT ISOMETRY OUTPUT.*
2. *Conversely, (α,β,ℓ)-PURE PRODUCT ISOMETRY OUTPUT trivially reduces to both $(\alpha,\beta^2/16,\ell)$-PRODUCT ISOMETRY OUTPUT and $(\alpha,\beta^2/16,\ell)$-SEPARABLE ISOMETRY OUTPUT.*

Proof. By definition, no-instances of both (α,β,ℓ)-PRODUCT ISOMETRY OUTPUT and (α,β,ℓ)-SEPARABLE ISOMETRY OUTPUT are also no-instances of $(4\sqrt{\alpha},\beta,\ell)$-PURE PRODUCT ISOMETRY OUTPUT. By Proposition 6.7, yes-instances of both (α,β,ℓ)-PRODUCT ISOMETRY OUTPUT and (α,β,ℓ)-SEPARABLE ISOMETRY OUTPUT are also yes-instances of $(4\sqrt{\alpha},\beta,\ell)$-PURE PRODUCT ISOMETRY OUTPUT.

By definition, yes-instances of (α,β,ℓ)-PURE PRODUCT ISOMETRY OUTPUT are also yes-instances of both $(\alpha,\beta^2/16,\ell)$-PRODUCT ISOMETRY OUTPUT and $(\alpha,\beta^2/16,\ell)$-SEPARABLE ISOMETRY OUTPUT. By the contrapositive of Proposition 6.7, no-instances of (α,β,ℓ)-PURE PRODUCT ISOMETRY OUTPUT are also no-instances of both $(\alpha,\beta^2/16,\ell)$-PRODUCT ISOMETRY OUTPUT and $(\alpha,\beta^2/16,\ell)$-SEPARABLE ISOMETRY OUTPUT. □

Corollary 6.9 (QMA(2)-completeness of equivalent problems). *The following hold:*

1. *Problems 6.5 and 6.6 are in QMA(2) for all ℓ and all $\alpha < \beta^2/16$.*
2. *These two problems are QMA(2)-hard for all $\ell \ge 2$ and all $(\alpha,\beta) = (\varepsilon, 1/4-\varepsilon)$, even when ε decays exponentially in the input length.*

Thus, these two problems are QMA(2)-complete for all $\ell \ge 2$ if both $0 < \alpha < \beta^2/16$ and $\beta < 1/4$.

Remark 6.10. The fact that Problems 6.5 and 6.6 are QMA(2)-hard only for $(\alpha,\beta) = (\varepsilon, 1/4-\varepsilon)$ instead of the best possible $(\varepsilon, 2-\varepsilon)$ is an artifact of Proposition 6.7. The best possible hardness result would be obtained if the bound in Proposition 6.7 could somehow be improved from $4\sqrt{\delta}$ to $\sqrt{2\delta}$.

7 PRODUCT STATE is QSZK-complete

In this section we prove QSZK-completeness of the problem of determining whether the state prepared by a given quantum circuit is close to a product state.

Problem 7.1 ((α,β)-PRODUCT STATE)**.**

Input: A description of a quantum circuit that prepares an ℓ-partite mixed state ρ.

Yes: ρ is α-close to a product state:

$$\min_{\rho}\min_{\sigma_1,\ldots,\sigma_\ell}\|\rho-\sigma_1\otimes\cdots\otimes\sigma_\ell\|_1\leq\alpha. \tag{7.1}$$

No: ρ is β-far from product:

$$\min_{\rho}\min_{\sigma_1,\ldots,\sigma_\ell}\|\rho-\sigma_1\otimes\cdots\otimes\sigma_\ell\|_1\geq\beta. \tag{7.2}$$

The main result of this section is the following theorem:

Theorem 7.2 (PRODUCT STATE is QSZK-complete)**.** *The following hold:*

1. (α,β,ℓ)-PRODUCT STATE *is in* QSZK *for all ℓ and all $\alpha<\beta^2/(\ell+1)$.*
2. $(\varepsilon,2-\varepsilon)$-BIPARTITE PRODUCT STATE *is* QSZK*-hard, even when ε decays exponentially in the input length.*

Thus, the problem is QSZK*-complete for all $\ell\geq 2$ and all $0<\alpha<\beta^2/(\ell+1)$ and $\beta<2$.*

This result is proven by establishing equivalence between the PRODUCT STATE problem and the QUANTUM STATE SIMILARITY problem, which is defined as follows:

Problem 7.3 ((α,β)-QUANTUM STATE SIMILARITY)**.**

Input: Descriptions of two quantum circuits that prepare mixed states ρ_0,ρ_1.

Yes: ρ_0 and ρ_1 are α-close: $\|\rho_0-\rho_1\|_1\leq\alpha$.

No: ρ_0 and ρ_1 are β-far apart: $\|\rho_0-\rho_1\|_1\geq\beta$.

Problem 7.3 is known to be QSZK-complete. Specifically, (α,β)-QUANTUM STATE SIMILARITY is contained in QSZK for all $\alpha<\beta^2$ and $(\varepsilon,2-\varepsilon)$-QUANTUM STATE SIMILARITY is QSZK-hard, even when ε decays exponentially in the input length [70, 74]. Thus, Theorem 7.2 can be proved by reducing Problems 7.1 and 7.3 to each other.

7.1 Containment in QSZK

Our reduction from PRODUCT STATE to QUANTUM STATE SIMILARITY employs the fact that if ρ is close to a product state then ρ is also close to the product of its reduced states. We are not aware of an explicit proof of this fact in the literature, so we provide a proof.

Lemma 7.4 (Approximation by a product of reduced states)**.** *Let ρ be a state of registers $A_1,\dots,A_\ell$ and suppose there is a product state $\sigma_1\otimes\cdots\otimes\sigma_\ell$ with*

$$\|\rho-\sigma_1\otimes\cdots\otimes\sigma_\ell\|_1\le\alpha\,. \tag{7.3}$$

Then it follows that

$$\|\rho-\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}\|_1\le(\ell+1)\alpha \tag{7.4}$$

where ρ_{A_i} denotes the reduced state of ρ on register A_i for $i=1,\dots,\ell$.

Proof. By the triangle inequality we have

$$\|\rho-\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}\|_1\le\|\rho-\sigma_1\otimes\cdots\otimes\sigma_\ell\|_1+\|\sigma_1\otimes\cdots\otimes\sigma_\ell-\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}\|_1. \tag{7.5}$$

By assumption the first term on the right is no larger than α. For the second term, another application of the triangle inequality yields

$$\begin{aligned}
&\|\sigma_1\otimes\cdots\otimes\sigma_\ell-\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}\|_1 &(7.6)\\
\le\;&\|\sigma_1\otimes\cdots\otimes\sigma_\ell-\rho_{A_1}\otimes\sigma_2\otimes\cdots\otimes\sigma_\ell\|_1+\|\rho_{A_1}\otimes\sigma_2\otimes\cdots\otimes\sigma_\ell-\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}\|_1 &(7.7)\\
=\;&\|\sigma_1-\rho_{A_1}\|_1+\|\sigma_2\otimes\cdots\otimes\sigma_\ell-\rho_{A_2}\otimes\cdots\otimes\rho_{A_\ell}\|_1\,. &(7.8)
\end{aligned}$$

By the contractivity of the trace norm under partial trace we have

$$\|\sigma_i-\rho_{A_i}\|_1\le\|\sigma_1\otimes\cdots\otimes\sigma_\ell-\rho\|_1\le\alpha \tag{7.9}$$

for each $i=1,\dots,\ell$. The lemma then follows by applying (7.6)-(7.8) inductively. □

We are now ready to reduce PRODUCT STATE to QUANTUM STATE SIMILARITY.

Proposition 7.5. *(α,β,ℓ)-*PRODUCT STATE *is in* QSZK *for all ℓ and all $\alpha<\beta^2/(\ell+1)$.*

Proof. We reduce (α,β,ℓ)-PRODUCT STATE to $((\ell+1)\alpha,\beta)$-QUANTUM STATE SIMILARITY. It then follows that (α,β,ℓ)-PRODUCT STATE is in QSZK whenever $\alpha<\beta^2/(\ell+1)$ as desired.

The reduction is as follows: given an instance ρ of (α,β,ℓ)-PRODUCT STATE, one can construct circuits that prepare states

$$\begin{aligned}
\rho_0&=\rho\,, &(7.10)\\
\rho_1&=\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}. &(7.11)
\end{aligned}$$

Specifically, we use the original circuit to make $\rho_0=\rho$, and we use the original circuit ℓ times to make ℓ copies of ρ and then trace over the appropriate subsystems to make $\rho_1=\rho_{A_1}\otimes\cdots\otimes\rho_{A_\ell}$. If ρ is a yes-instance of (α,β,ℓ)-PRODUCT STATE then by Lemma 7.4 we have that $\|\rho_0-\rho_1\|_1\le(\ell+1)\alpha$. Conversely, if ρ is a no-instance of (α,β,ℓ)-PRODUCT STATE then it must be that $\|\rho_0-\rho_1\|_1\ge\beta$. □

7.2 Hardness for QSZK

Proposition 7.6. $(\varepsilon, 2-\varepsilon)$-BIPARTITE PRODUCT STATE *is* QSZK*-hard, even when ε decays exponentially in the input length.*

Proof. We reduce $(\delta, 2-\delta)$-QUANTUM STATE SIMILARITY to (α, β)-BIPARTITE PRODUCT STATE for

$$\alpha = n\delta/2\,, \tag{7.12}$$

$$\beta = 2 - 2^{-\Omega(n)}\,, \tag{7.13}$$

for any desired n. The desired hardness result then follows by an appropriate choice of δ, n.

The reduction is as follows. Given an instance (ρ_0, ρ_1) of QUANTUM STATE SIMILARITY we construct a circuit that prepares n copies of the bipartite state $\omega_{A:S}$ of registers AS given by

$$\omega_{A:S} = \frac{1}{2}|0\rangle\langle 0|_A \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1|_A \otimes \rho_1\,. \tag{7.14}$$

Figure 5 illustrates an isometric circuit for preparing (a purification of) a single copy of $\omega_{A:S}$.

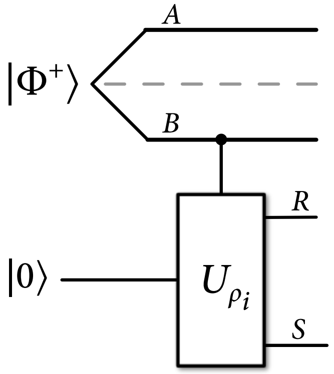


Figure 5: The isometric circuit that prepares a purification of $\omega_{A:S}$. This circuit is produced by our reduction from QUANTUM STATE SIMILARITY to BIPARTITE PRODUCT STATE. Here U_{ρ_i} are the unitary circuits that prepare $\rho_i = \mathrm{Tr}_R(U_{\rho_i}|0\rangle\langle 0|U^*_{\rho_i})$ in register S for $i \in \{0,1\}$. This same circuit is also produced by the reduction of [46] from QUANTUM STATE DISTINGUISHABILITY to the one-way LOCC version of SEPARABLE STATE, except that reduction discards register S instead of R.

If (ρ_0, ρ_1) is a yes-instance of $(\delta, 2-\delta)$-QUANTUM STATE SIMILARITY then the trace distance between $\omega_{A:S}$ and the product state

$$\sigma_{A:S} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)_A \otimes \rho_0 \tag{7.15}$$

is at most $(1/2)\|\rho_0 - \rho_1\|_1 \leq \delta/2$. It then follows from [70, Lemma 8] that

$$\left\|\omega_{A:S}^{\otimes n} - \sigma_{A:S}^{\otimes n}\right\|_1 \leq n\delta/2\,. \tag{7.16}$$

As $\sigma_{A:S}^{\otimes n}$ is a product relative to the bipartite cut $A_1 \cdots A_n : S_1 \cdots S_n$ it must be that $\omega_{A:S}^{\otimes n}$ is a yes-instance of (α, β)-BIPARTITE PRODUCT STATE relative to this cut.

By contrast, if (ρ_0, ρ_1) is a no-instance of $(\delta, 2-\delta)$-QUANTUM STATE SIMILARITY then $\omega_{A:S}$ is almost perfectly correlated on $A : S$ and hence far from a product. Recall that trace distance is equal to the maximum probability of distinguishing states over all possible measurements, 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 (register A) in the computational basis and by performing the Helstrom measurement $\{\Pi_0, \Pi_1\}$ on the second system, 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 $\omega_{A:S}$:

$$\omega'_{A:S'} = \frac{1}{2}\mathrm{Tr}\{\Pi_0\rho_0\}|00\rangle\langle 00| + \frac{1}{2}\mathrm{Tr}\{\Pi_1\rho_1\}|11\rangle\langle 11| + \frac{1}{2}\mathrm{Tr}\{\Pi_0\rho_1\}|10\rangle\langle 10| + \frac{1}{2}\mathrm{Tr}\{\Pi_1\rho_0\}|01\rangle\langle 01| . \tag{7.17}$$

Recall that the Helstrom measurement distinguishes two states ρ_0 and ρ_1 with the following success probability:

$$\frac{1}{2}\mathrm{Tr}\{\Pi_0\rho_0\} + \frac{1}{2}\mathrm{Tr}\{\Pi_1\rho_1\} = \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_0 - \rho_1\|_1\right), \tag{7.18}$$

and the following error probability:

$$\frac{1}{2}\mathrm{Tr}\{\Pi_0\rho_1\} + \frac{1}{2}\mathrm{Tr}\{\Pi_1\rho_0\} = \frac{1}{2}\left(1 - \frac{1}{2}\|\rho_0 - \rho_1\|_1\right). \tag{7.19}$$

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

$$\overline{\Phi}_{A:S'} := \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|), \tag{7.20}$$

is no larger than

$$1 - \frac{1}{2}\|\rho_0 - \rho_1\|_1 \leq \frac{\delta}{2}. \tag{7.21}$$

For 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 $|0\rangle\langle 0|$ and the probability q of measuring Π_0:

$$\sigma_{p,q} = pq|00\rangle\langle 00| + p(1-q)|01\rangle\langle 01| + q(1-p)|10\rangle\langle 10| + (1-p)(1-q)|11\rangle\langle 11| . \tag{7.22}$$

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

$$\min_{\sigma_0,\sigma_1}\|\sigma_0 \otimes \sigma_1 - \omega_{A:S}\|_1 \geq \min_{p,q}\|\sigma_{p,q} - \omega'_{A:S}\|_1 . \tag{7.23}$$

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

$$\begin{aligned}
\min_{p,q} \| \sigma_{p,q} - \omega'_{A:S} \|_1 &\geq \min_{p,q} \| \sigma_{p,q} - \overline{\Phi}_{A:S} \|_1 - \| \overline{\Phi}_{A:S} - \omega'_{A:S} \|_1 && (7.24)\\
&\geq \| \sigma_{p,q} - \overline{\Phi}_{A:S} \|_1 - \frac{\delta}{2} && (7.25)\\
&= \left| \frac{1}{2} - pq \right| + \left| \frac{1}{2} - (1-p)(1-q) \right| + |p(1-q)| + |q(1-p)| - \frac{\delta}{2} && (7.26)\\
&= \frac{1}{2} - pq + \left| \frac{1}{2} - (1-p)(1-q) \right| + p(1-q) + q(1-p) - \frac{\delta}{2} && (7.27)\\
&\geq \frac{1}{2} - pq + p(1-q) + q(1-p) - \frac{\delta}{2} && (7.28)\\
&\geq \frac{1}{2} + p(1-q) - \frac{\delta}{2} && (7.29)\\
&\geq \frac{1-\delta}{2}, && (7.30)
\end{aligned}$$

where the first line follows from the triangle inequality, and the fourth through last lines follow from the fact that $0 \leq p \leq 1/2$ and $0 \leq q \leq 1$. It then follows from [70, Lemma 8] that for suitably high n we have that $\omega_{A:S}^{\otimes n}$ is at least $\left(2 - 2^{-\Omega(n)}\right)$-far from any product state and so this state is a no-instance of (α, β)-BIPARTITE PRODUCT STATE as desired. □

Remark 7.7. Theorem 7.2 provides a different proof that the promise problem ERROR CORRECTABILITY of [42] is QSZK-complete (with a proof preceding this one given in [47]). 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-zero 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 [45], 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 7.2 that ERROR CORRECTABILITY and PRODUCT STATE are reducible to each another and that ERROR CORRECTABILITY is QSZK-complete.

8 A short quantum game for the one-way LOCC version of SEPARABLE STATE

In [46] it was shown that the one-way LOCC version of the SEPARABLE STATE problem admits a two-message quantum interactive proof, 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 1.1, this result is not a complexity-theoretic improvement over prior work. But it is interesting that the one-way LOCC version of SEPARABLE STATE admits a natural, single-message quantum proof provided that the verifier has help from a second competing prover. Recall the definition of the one-way LOCC version of the SEPARABLE STATE problem [46]:

Problem 8.1 ((α,β,ℓ)-SEPARABLE STATE, one-way LOCC version)**.**

Input: A description of a quantum circuit that prepares a state ρ of registers $A_1 \cdots A_\ell$.

Yes: ρ is α-close in trace distance to a separable state:

$$\min_{\sigma \in \mathcal{S}(A_1:\cdots:A_\ell)} \|\rho - \sigma\|_1 \leq \alpha\,. \tag{8.1}$$

No: ρ is β-far in one-way LOCC distance from separable:

$$\min_{\sigma \in \mathcal{S}(A_1:\cdots:A_\ell)} \|\rho - \sigma\|_{\text{1-LOCC}} \geq \beta\,. \tag{8.2}$$

The main result of this section is the following proposition:

Proposition 8.2. *The one-way LOCC version of* (α,β,ℓ)-SEPARABLE STATE *is in* SQG *for all* ℓ *and all* $\alpha < \beta$.

Proof. Suppose that registers $A_1 \cdots A_\ell$ have combined total dimension D. The verifier witnessing membership of the problem in SQG is described as follows:

1. Receive $k\ell$ registers from the yes-prover labeled A_i^j for $i = 1,\ldots,\ell$ and $j = 1,\ldots,k$ where

$$k = \left\lceil \ell + \frac{16\ell^2 \log D}{(\beta-\alpha)^2} \right\rceil . \tag{8.3}$$

(Intuitively, these registers contain a purported k-extension of ρ.)

2. Perform ℓ permutation tests: one for each group $(A_i^1,\ldots,A_i^k)$ of k registers. Reject immediately if any test fails. Discard all registers except $A_1^1,\ldots,A_\ell^1$, letting σ denote the reduced state of these remaining registers.

3. Prepare a copy of ρ using the input circuit and choose a random bit $b \in \{0,1\}$. If $b = 0$ then send ρ to the no-prover. Otherwise, send σ to the no-prover. (Intuitively, the no-prover is challenged to identify whether the state he receives from the verifier is ρ or σ.)

4. Receive a single bit b' from the no-prover. Reject 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 σ that is α-close in trace distance to ρ and send the verifier a k-extension of σ. As σ is separable, such an 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 σ from ρ, which he can do with probability no larger than $1/2 + \alpha/4$, implying that the verifier accepts with probability at least $1/2 - \alpha/4$.

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

$$\frac{1}{2}+\frac{1}{4}\min_{\sigma\in\mathcal{E}_k}\|\rho-\sigma\|_1 . \tag{8.4}$$

(The existence of such a measurement was first shown in [40] and a simple proof can be found in Yu, Duan, and Xu [80].)

To see that the yes-prover cannot win, observe that if the permutation test of step 2 passes then the state of all $k\ell$ registers A_i^j received from the yes-prover is projected into the symmetric subspaces of $(A_i^1,\ldots,A_i^k)$ for each $i=1,\ldots,\ell$. The set of such states is contained in the set $\mathcal{E}_k$ of k-extendible states, and we know from Theorem 5.3 and our choice of k that

$$\min_{\sigma\in\mathcal{E}_k}\|\rho-\sigma\|_1 \geq \frac{\beta+\alpha}{2} . \tag{8.5}$$

Thus, the no-prover convinces the verifier to reject with probability at least $1/2+(\beta+\alpha)/8$, implying that the verifier accepts with probability at most $1/2-(\beta+\alpha)/8$. This protocol witnesses membership in SQG whenever $1/2-\alpha/4 > 1/2-(\beta+\alpha)/8$, which occurs whenever $\alpha<\beta$. □

9 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 [75, 23] and references therein. This is also the case with the work in [44] and we comment briefly on this connection. The original definition of the geometric measure of entanglement for a pure state $|\psi\rangle$ of registers AB is defined as the maximum squared overlap with a pure product state:

$$\max_{|\phi\rangle_A,|\varphi\rangle_B} |\langle\phi\otimes\varphi|\psi\rangle|^2 . \tag{9.1}$$

This quantity has an operational interpretation as the maximum probability with which the state $|\psi\rangle$ would pass a test for being a pure product state. By taking the negative logarithm one obtains an entropic-like quantity that is equal to the geometric measure of entanglement and satisfies a list of desirable requirements that any entanglement measure ought to meet.

If one has a promise that the quantity (9.1) is larger than $1-\varepsilon$ or smaller than ε (as in the definition of the PURE PRODUCT STATE problem, Problem 4.1) then the product test can be used to determine which is the case. However, this observation does not directly give an operational interpretation of the quantity in (9.1). Rather, an operational interpretation of (9.1) is given by the quantum interactive proof in [46] for SEPARABLE STATE, whose maximum acceptance probability for a given state ρ of registers AB is given by

$$\max_{\sigma\in\mathcal{S}(A:B)} F(\rho_{AB},\sigma_{AB}) , \tag{9.2}$$

of which (9.1) is a special case when ρ_{AB} is pure. (This bound holds in the limit of large k, the number of registers sent by the prover in a purported k-extension of ρ.) The operational interpretation for (9.2) is that it is the maximum probability with which a prover could convince a verifier that a state ρ is separable by acting on a purification of ρ.

Our work has also unveiled and provided operational interpretations for other quantifiers of entanglement that fall within the geometric class. Indeed, the maximum acceptance probability of our quantum witness for the one-way LOCC version of SEPARABLE ISOMETRY OUTPUT is bounded by

$$\max_{\rho,\,\sigma_{AB}\in\mathcal{S}} F(U(\rho_S\otimes|0\rangle\langle 0|)U^\dagger,\sigma_{AB})\,, \tag{9.3}$$

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 [81], that is, its ability to take a product state input to an entangled output no matter what the input is. Furthermore, the quantum interactive proof for the one-way LOCC version of SEPARABLE CHANNEL OUTPUT given in [46] has the following upper bound on its maximum acceptance probability:

$$\max_{\rho,\,\sigma_{AB}\in\mathcal{S}} F(\mathcal{N}_{S\to AB}(\rho_S),\sigma_{AB})\,, \tag{9.4}$$

where $\mathcal{N}_{S\to AB}$ 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 the quantum interactive proof provides an operational interpretation for the above quantity as well.

10 Discussion: Does nondeterminism trump one-way LOCC distance?

An interesting and surprising comparison emerges in light of the combined results of the present paper with those of [46]. For isometric channels, it is no surprise that detecting product outputs is easier than detecting separable outputs when no-instances in the former problem are promised to be far from a product in one-way LOCC distance instead of trace distance: these problems are complete for QMA and QMA(2), respectively. For states, however, detecting separability is *harder* than detecting productness, *even when no-instances in the former problem are promised to be far from separable in one-way LOCC distance:* the former is both QSZK- and NP-hard while the latter is QSZK-complete.

An anonymous reviewer suggests one possible explanation for this phenomenon: the added difficulty of nondeterminism trumps the reduced difficulty of the one-way LOCC promise. Specifically, detecting entangled or correlated isometry outputs is inherently "nondeterministic," as one must guess the proper input to the isometry. Similarly, detecting separable states is also "nondeterministic," as one must guess a mixture of product states. By contrast, product states have no nondeterminism of this form and so we can expect the corresponding detection problem to be easier, even when one demands a lower error tolerance via the trace distance.

This explanation is interesting and intuitive. To this explanation we add the following observation: even product states contain "nondeterminism" in the sense that we must also recognize products of *mixed* states, not just pure states, and that the PURE PRODUCT STATE problems (both one-way LOCC and trace distance versions) are even easier (BQP-complete).

11 Conclusion

We have proved that several separability testing problems are complete for BQP, QMA, QMA(2), and QSZK. These completeness results build upon the work of [46], which exhibits a separability testing problem in QIP(2) and another problem complete for QIP. The completeness of these 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 entanglement-related problems 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 interactive proof classes. Some patterns emerge: it seems as though mixed state separability requires two messages to be added onto a proof for pure state separability so that the prover may act upon the purification of the mixed state, as is the case for both the "state" and "channel" versions of these problems.

Two-message quantum interactive proofs continue to be somewhat mysterious. Extrapolating from our results, the one-way LOCC version of SEPARABLE STATE has the qualities that one would intuitively expect of a QIP(2)-complete problem. Despite this intuition, we do not know whether it is QIP(2)-complete or even QMA-hard. However, our work here provides some intuition for why the problem should not be either QSZK- or QMA-complete—there are other problems very different from it that are complete for these classes.

Our work can be extended in a number of directions. The trace distance version of SEPARABLE CHANNEL OUTPUT may help to understand the relation between multi-prover quantum interactive proofs with and without entanglement among the provers (QMIP versus QMIP*). Similarly, the trace distance version of SEPARABLE STATE may provide further insights. It would also be worthwhile to characterize the channel version of PRODUCT STATE in order to map out more of the space of separability testing problems. Such an extension may also help to provide a tighter characterization of classes that rely on "unentanglement," such as QMA(2).

It is satisfying that each of the separability testing problems (with the possible exception of the one-way LOCC version of SEPARABLE STATE) is complete for a different complexity class. Perhaps by studying the remaining related problems and their variants (trace norm versus one-way LOCC norm, separable states versus product states, *etc.*) one may find two different separability testing problems that are nontrivially reducible to each other.

Acknowledgements

We thank Claude Crépeau, Brian Swingle, and John Watrous for helpful conversations and the anonymous referees for many helpful suggestions. 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. MMW began this project while affiliated with the School of Computer Science, McGill University.

References

[1] SCOTT AARONSON: *Quantum Computing since Democritus*. Cambridge Univ. Press, 2013. 62

[2] SCOTT AARONSON, SALMAN BEIGI, ANDREW DRUCKER, BILL FEFFERMAN, AND PETER SHOR: The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009. Preliminary version in CCC'08. [doi:10.4086/toc.2009.v005a001] 67

[3] ANDRIS AMBAINIS, ADAM SMITH, AND KE YANG: Extracting quantum entanglement (general entanglement purification protocols). In *Proc. 17th IEEE Conf. on Computational Complexity (CCC'02)*, pp. 82–91, 2002. [doi:10.1109/CCC.2002.1004345, arXiv:quant-ph/0110011] 61, 69

[4] LÁSZLÓ BABAI: Trading group theory for randomness. In *Proc. 17th STOC*, pp. 421–429. ACM Press, 1985. [doi:10.1145/22145.22192] 60

[5] LÁSZLÓ BABAI AND SHLOMO MORAN: Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Comput. System Sci.*, 36(2):254–276, 1988. [doi:10.1016/0022-0000(88)90028-1] 60

[6] ADRIANO BARENCO, ANDRE BERTHIAUME, DAVID DEUTSCH, ARTUR EKERT, RICHARD JOZSA, AND CHIARA MACCHIAVELLO: Stabilization of quantum computations by symmetrization. *SIAM J. Comput.*, 26(5):1541–1557, 1997. [doi:10.1137/S0097539796302452, arXiv:quant-ph/9604028] 65

[7] HOWARD BARNUM, CLAUDE CRÉPEAU, DANIEL GOTTESMAN, ADAM SMITH, AND ALAIN TAPP: Authentication of quantum messages. In *Proc. 43rd FOCS*, pp. 449–458. IEEE Comp. Soc. Press, 2002. [doi:10.1109/SFCS.2002.1181969, arXiv:quant-ph/0205128] 61, 69

[8] SALMAN BEIGI: NP vs $\mathsf{QMA}_{\log}(2)$. *Quantum Inf. Comput.*, 10(1&2):141–151, 2010. [arXiv:0810.5109] 67

[9] 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, 1993. [doi:10.1103/PhysRevLett.70.1895] 60

[10] CHARLES H. BENNETT, DAVID P. DIVINCENZO, JOHN A. SMOLIN, AND WILLIAM K. WOOTTERS: Mixed state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, 1996. [doi:10.1103/PhysRevA.54.3824, arXiv:quant-ph/9604024] 61, 69

[11] 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, 1999. [doi:10.1103/PhysRevLett.83.3081, arXiv:quant-ph/9904023] 60

[12] 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 Trans.*

Inform. Theory, 48(10):2637–2655, 2002. [doi:10.1109/TIT.2002.802612, arXiv:quant-ph/0106052] 60

[13] 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, 1992. [doi:10.1103/PhysRevLett.69.2881] 60

[14] DOMINIC W. BERRY, GRAEME AHOKAS, RICHARD CLEVE, AND BARRY C. SANDERS: Efficient quantum algorithms for simulating sparse Hamiltonians. *Communications in Mathematical Physics*, 270(2):359–371, 2007. [doi:10.1007/s00220-006-0150-x, arXiv:quant-ph/0508139] 60

[15] HUGUE BLIER AND ALAIN TAPP: All languages in NP have very short quantum proofs. In *Third International Conference on Quantum, Nano and Micro Technologies, 2009. ICQNM '09.*, pp. 34–37, 2009. [doi:10.1109/ICQNM.2009.21, arXiv:0709.0738] 67

[16] FERNANDO G. S. L. BRANDÃO AND MATTHIAS CHRISTANDL: Detection of multiparticle entanglement: Quantifying the search for symmetric extensions. *Physical Review Letters*, 109(16):160502, 2012. [doi:10.1103/PhysRevLett.109.160502, arXiv:1105.5720] 66

[17] FERNANDO G. S. L. BRANDÃO, MATTHIAS CHRISTANDL, AND JON YARD: Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, 2011. [doi:10.1007/s00220-011-1302-1, arXiv:1010.1750] 61

[18] FERNANDO G. S. L. BRANDÃO, MATTHIAS CHRISTANDL, AND JON YARD: A quasipolynomial-time algorithm for the quantum separability problem. In *Proc. 43rd STOC*, pp. 343–351. ACM Press, 2011. [doi:10.1145/1993636.1993683, arXiv:1011.2751] 67

[19] FERNANDO G. S. L. BRANDÃO AND ARAM WETTROTH HARROW: Quantum de Finetti theorems under local measurements with applications. In *Proc. 45th STOC*, pp. 861–870. ACM Press, 2013. [doi:10.1145/2488608.2488718, arXiv:1210.6367] 66, 74, 75

[20] HARRY BUHRMAN, RICHARD CLEVE, JOHN WATROUS, AND RONALD DE WOLF: Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001. [doi:10.1103/PhysRevLett.87.167902, arXiv:quant-ph/0102001] 65

[21] ANDRÉ CHAILLOUX AND OR SATTATH: The complexity of the separable Hamiltonian problem. In *Proc. 27th IEEE Conf. on Computational Complexity (CCC'12)*, pp. 32–41, 2012. [doi:10.1109/CCC.2012.42, arXiv:1111.5247] 67

[22] JING CHEN AND ANDREW DRUCKER: Short multi-prover quantum proofs for SAT without entangled measurements. 2010. [arXiv:1011.0716] 67

[23] LIN CHEN, MARTIN AULBACH, AND MICHAL HAJDUSEK: Comparison of different definitions of the geometric measure of entanglement. *Physical Review A*, 89(4):042305, 2014. [doi:10.1103/PhysRevA.89.042305, arXiv:1308.0806] 61, 92

[24] ALESSANDRO CHIESA AND MICHAEL A. FORBES: Improved soundness for QMA with multiple provers. *Chicago Journal of Theoretical Computer Science*, 2013, Article 1. [doi:10.4086/cjtcs.2013.001] 67

[25] RICHARD CLEVE AND HARRY BUHRMAN: Substituting quantum entanglement for communication. *Physical Review A*, 56(2):1201–1204, 1997. [doi:10.1103/PhysRevA.56.1201, arXiv:quant-ph/9704026] 60

[26] STEPHEN A. COOK: The complexity of theorem proving procedures. In *Proc. 3rd STOC*, pp. 151–158. ACM Press, 1971. [doi:10.1145/800157.805047] 60

[27] STEPHEN A. COOK AND PHUONG NGUYEN: *Logical Foundations of Proof Complexity*. Cambridge Univ. Press, 2010. [doi:10.1017/CBO9780511676277] 60

[28] TOBY S. CUBITT, DEBBIE LEUNG, WILLIAM MATTHEWS, AND ANDREAS WINTER: Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104(23):230503, 2010. [doi:10.1103/PhysRevLett.104.230503, arXiv:0911.5300] 60

[29] DAVID P. DIVINCENZO, PATRICK HAYDEN, AND BARBARA M. TERHAL: Hiding quantum data. *Foundations of Physics*, 33(11):1629–1647, 2003. [doi:10.1023/a:1026013201376, arXiv:quant-ph/0207147] 60

[30] DAVID P. DIVINCENZO, DEBBIE W. LEUNG, AND BARBARA M. TERHAL: Quantum data hiding. *IEEE Trans. Inform. Theory*, 48(3):580–598, March 2002. [doi:10.1109/18.985948, arXiv:quant-ph/0103098] 60

[31] ANDREW C. DOHERTY, PABLO A. PARRILO, AND FEDERICO M. SPEDALIERI: Distinguishing separable and entangled states. *Physical Review Letters*, 88(18):187904, 2002. [doi:10.1103/PhysRevLett.88.187904, arXiv:quant-ph/0112007] 74

[32] ANDREW C. DOHERTY, PABLO A. PARRILO, AND FEDERICO M. SPEDALIERI: Complete family of separability criteria. *Physical Review A*, 69(2):022308, 2004. [doi:10.1103/PhysRevA.69.022308, arXiv:quant-ph/0308032] 74

[33] ANDREW C. DOHERTY, PABLO A. PARRILO, AND FEDERICO M. SPEDALIERI: Detecting multipartite entanglement. *Physical Review A*, 71(3):032333, 2005. [doi:10.1103/PhysRevA.71.032333] 74

[34] TILO EGGELING AND REINHARD F. WERNER: Hiding classical data in multipartite quantum states. *Physical Review Letters*, 89(9):097905, 2002. [doi:10.1103/physrevlett.89.097905, arXiv:0203004] 60

[35] ARTUR K. EKERT: Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991. [doi:10.1103/PhysRevLett.67.661] 60

[36] CHRISTOPHER A. FUCHS AND JEROEN VAN DE GRAAF: Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inform. Theory*, 45(4):1216, 1999. [doi:10.1109/18.761271, arXiv:quant-ph/9712042] 65

[37] SEVAG GHARIBIAN: Strong NP-hardness of the quantum separability problem. *Quantum Inf. Comput.*, 10(3):343–360, 2010. [arXiv:0810.4507] 60

[38] SHAFI GOLDWASSER, SILVIO MICALI, AND CHARLES RACKOFF: The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989. Preliminary version in STOC'85. [doi:10.1137/0218012] 60

[39] LEONID GURVITS: Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proc. 35th STOC*, pp. 10–19. ACM Press, 2003. [doi:10.1145/780542.780545, arXiv:quant-ph/0303055] 60

[40] GUS GUTOSKI AND JOHN WATROUS: Quantum interactive proofs with competing provers. In *Proc. 22nd Symp. Theoretical Aspects of Comp. Sci. (STACS'05)*, volume 3404 of *LNCS*, pp. 605–616. Springer, 2005. [doi:10.1007/978-3-540-31856-9_50, arXiv:cs/0412102] 68, 92

[41] GUS GUTOSKI AND XIAODI WU: Parallel approximation of min-max problems. *Comput. Complexity*, 22(2):385–428, 2013. Preliminary version in CCC'12. [doi:10.1007/s00037-013-0065-9, arXiv:1011.2787] 62, 68

[42] DANIEL HARLOW AND PATRICK HAYDEN: Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013(6):85, 2013. [doi:10.1007/JHEP06(2013)085, arXiv:1301.4504] 90

[43] ARAM WETTROTH HARROW AND DEBBIE LEUNG: A communication-efficient nonlocal measurement with application to communication complexity and bipartite gate capacities. *IEEE Trans. Inform. Theory*, 57(8):5504–5508, 2011. [doi:10.1109/TIT.2011.2158468, arXiv:0803.3066] 61, 69

[44] ARAM WETTROTH HARROW AND ASHLEY MONTANARO: An efficient test for product states with applications to quantum Merlin-Arthur games. In *Proc. 51st FOCS*, pp. 633–642. IEEE Comp. Soc. Press, 2010. [doi:10.1109/FOCS.2010.66, arXiv:1001.0017] 61, 62, 67, 68, 71, 81, 92

[45] PATRICK HAYDEN, MICHAL HORODECKI, ANDREAS WINTER, AND JON YARD: A decoupling approach to the quantum capacity. *Open Systems & Information Dynamics*, 15(1):7–19, 2008. [doi:10.1142/S1230161208000043, arXiv:quant-ph/0702005] 90

[46] PATRICK HAYDEN, KEVIN MILNER, AND MARK M. WILDE: Two-message quantum interactive proofs and the quantum separability problem. *Quantum Inf. Comput.*, 14(5 & 6):384–416, 2014. Preliminary version at CCC'13. [arXiv:1211.6120] 60, 61, 62, 63, 77, 88, 90, 91, 92, 93, 94

[47] PATRICK HAYDEN AND BRIAN SWINGLE: Quantum error correction and QSZK. unpublished, 2012. 90

[48] CARL W. HELSTROM: Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969. [doi:10.1007/BF01007479] 64

[49] RYSZARD HORODECKI, PAWEŁ HORODECKI, MICHAŁ HORODECKI, AND KAROL HORODECKI: Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, 2009. [doi:10.1103/RevModPhys.81.865, arXiv:quant-ph/0702225] 60, 70

[50] RAHUL JAIN, ZHENGFENG JI, SARVAGYA UPADHYAY, AND JOHN WATROUS: QIP = PSPACE. *J. ACM*, 58(6):30, 2011. Preliminary version in STOC'10. [doi:10.1145/2049697.2049704] 62, 67

[51] RAHUL JAIN, SARVAGYA UPADHYAY, AND JOHN WATROUS: Two-message quantum interactive proofs are in PSPACE. In *Proc. 50th FOCS*, pp. 534–543. IEEE Comp. Soc. Press, 2009. [doi:10.1109/FOCS.2009.30, arXiv:0905.1300] 62, 68, 76

[52] 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, 2008. [doi:10.1088/1751-8113/41/39/395309, arXiv:0809.2037] 65

[53] ALEXEI YU. KITAEV: Quantum measurements and the Abelian Stabilizer Problem. *ECCC*, TR96-003, 1995. [arXiv:quant-ph/9511026] 65

[54] ALEXEI YU. KITAEV AND JOHN WATROUS: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proc. 32nd STOC*, pp. 608–617. ACM Press, 2000. [doi:10.1145/335305.335387] 60, 67, 68

[55] HIROTADA KOBAYASHI AND KEIJI MATSUMOTO: Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. System Sci.*, 66(3):429–450, May 2003. Preliminary version in ISAAC'02. [doi:10.1016/s0022-0000(03)00035-7, arXiv:cs/0102013] 67

[56] CÉCILIA LANCIEN AND ANDREAS WINTER: Distinguishing multi-partite states by local measurements. *Communications in Mathematical Physics*, 323(2):555–573, 2013. [doi:10.1007/s00220-013-1779-x, arXiv:1206.2884] 66

[57] FRANÇOIS LE GALL, SHOTA NAKAGAWA, AND HARUMICHI NISHIMURA: On QMA protocols with two short quantum proofs. *Quantum Inf. Comput.*, 12(7&8):589–600, 2012. [arXiv:1108.4306] 67

[58] YI-KAI LIU, MATTHIAS CHRISTANDL, AND FRANK VERSTRAETE: Quantum computational complexity of the *N*-representability problem: QMA complete. *Physical Review Letters*, 98(11):110503, 2007. [doi:10.1103/PhysRevLett.98.110503, arXiv:quant-ph/0609125] 67

[59] SETH LLOYD: Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996. [doi:10.1126/science.273.5278.1073] 60

[60] CARSTEN LUND, LANCE FORTNOW, HOWARD KARLOFF, AND NOAM NISAN: Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992. Preliminary version in FOCS'90. [doi:10.1145/146585.146605] 68

[61] CHRIS MARRIOTT AND JOHN WATROUS: Quantum Arthur-Merlin games. *Comput. Complexity*, 14(2):122–152, 2005. Preliminary version in CCC'04. [doi:10.1007/s00037-005-0194-x, arXiv:cs/0506068] 68

[62] 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, 2009. [doi:10.1007/s00220-009-0890-5, arXiv:0810.2327] 60, 61, 66

[63] MICHAEL A. NIELSEN AND ISAAC L. CHUANG: *Quantum Computation and Quantum Information*. Cambridge Univ. Press, 2000. 62, 77

[64] CHRISTOS H. PAPADIMITRIOU: *Computational Complexity*. Addison-Wesley, 1994. 60

[65] ADI SHAMIR: IP = PSPACE. *J. ACM*, 39(4):869–877, 1992. Preliminary version in FOCS'90. [doi:10.1145/146585.146609] 68

[66] YAOYUN SHI AND XIAODI WU: Epsilon-net method for optimizations over separable states. In *Proc. 39th Internat. Colloq. on Automata, Languages and Programming (ICALP'12)*, volume 7391 of *LNCS*, pp. 798–809. Springer, 2012. [doi:10.1007/978-3-642-31594-7_67, arXiv:1112.0808] 67

[67] MICHAEL SIPSER: *Introduction to the Theory of Computation*. International Thomson Publishing, 1996. 60

[68] LARRY J. STOCKMEYER: The polynomial-time hierarchy. *Theoret. Comput. Sci.*, 3(1):1–22, 1976. [doi:10.1016/0304-3975(76)90061-X] 60

[69] UMESH VAZIRANI AND THOMAS VIDICK: Fully device independent quantum key distribution. *Physical Review Letters*, 113(14)(14):140501, 2014. [doi:10.1103/PhysRevLett.113.140501, arXiv:1210.1810] 60

[70] JOHN WATROUS: Limits on the power of quantum statistical zero-knowledge. In *Proc. 43rd FOCS*, pp. 459–468. IEEE Comp. Soc. Press, 2002. [doi:10.1109/SFCS.2002.1181970, arXiv:quant-ph/0202111] 62, 67, 68, 86, 88, 90

[71] JOHN WATROUS: PSPACE has constant-round quantum interactive proof systems. *Theoret. Comput. Sci.*, 292(3):575–588, 2003. Preliminary version in FOCS'99. [doi:10.1016/S0304-3975(01)00375-9] 60

[72] JOHN WATROUS: Theory of Quantum Information (course lecture notes). 2004. 69

[73] JOHN WATROUS: Quantum computational complexity. *Encyclopedia of Complexity and System Science*, pp. 7174–7201, 2009. [doi:10.1007/978-0-387-30440-3_428, arXiv:0804.3401] 60, 62

[74] JOHN WATROUS: Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version in STOC'06. [doi:10.1137/060670997, arXiv:quant-ph/0511020] 62, 67, 86

[75] TZU-CHIEH WEI AND PAUL M. GOLDBART: Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Physical Review A*, 68(4)(4):042307, 2003. [doi:10.1103/PhysRevA.68.042307, arXiv:quant-ph/0307219] 61, 92

[76] REINHARD F. WERNER: An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17(4):359–363, 1989. [doi:10.1007/BF00399761] 74

[77] REINHARD F. WERNER: Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, 1989. [doi:10.1103/PhysRevA.40.4277] 62

[78] MARK M. WILDE: *From Classical to Quantum Shannon Theory*. 2011. Published in [79]. [arXiv:1106.1445] 62

[79] MARK M. WILDE: *Quantum Information Theory*. Cambridge Univ. Press, 2013. 62, 101

[80] 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. 2012. [arXiv:1201.1172] 92

[81] PAOLO ZANARDI, CHRISTOF ZALKA, AND LARA FAORO: Entangling power of quantum evolutions. *Physical Review A*, 62(3):030301, 2000. [doi:10.1103/PhysRevA.62.030301, arXiv:quant-ph/0005031] 93

AUTHORS

Gus Gutoski
Postdoctoral Scholar
Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada
ggutoski@perimeterinstitute.ca
http://www.perimeterinstitute.ca/personal/ggutoski/

Patrick Hayden
Professor of Physics
Department of Physics, Stanford University, Stanford, California, USA
phayden@stanford.edu
http://web.stanford.edu/~phayden

Kevin Milner
Ph. D. student
University of Oxford, Oxford, UK
kamilner@kamilner.ca

Mark M. Wilde
Assistant Professor
Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana, USA
mwilde@lsu.edu
http://www.markwilde.com

ABOUT THE AUTHORS

GUS GUTOSKI was born in Kitchener, Ontario, twin city of Waterloo, Ontario. After completing a BMath at the University of Waterloo he briefly escaped the Region of Waterloo for a MSc at the University of Calgary in Calgary, Alberta. Unfortunately, his graduate advisor, John Watrous, subsequently took a position at the University of Waterloo. Gus reluctantly followed his advisor back to his hometown and completed a Ph. D. in Computer Science at the University of Waterloo. He is currently a postdoctoral researcher at the Perimeter Institute for Theoretical Physics in Waterloo and he cannot get enough of Waterloo. Gus's research interests include quantum complexity theory, quantum cryptography, and, lately, Bitcoin.

PATRICK HAYDEN received his D. Phil. in Physics from the University of Oxford in 2001 under the supervision of Artur Ekert. Subsequently he was a postdoc at Caltech before joining the faculty at McGill University, where he spent nine happy years before moving to Stanford in 2013. Like many computer scientists, Hayden developed an interest in complexity theory because of its possible relevance to black hole physics. His other research interests include skiing and backcountry camping. Outside of work, Hayden enjoys proving theorems in quantum communication theory and studying the emergence of spacetime.

KEVIN MILNER did his undergraduate studies at the University of Alberta where he developed an interest in complexity theory before joining McGill University to study quantum information for his M. Sc., under the supervision of Patrick Hayden. His hobbies include breaking and fixing the Internet, which he now studies as a D. Phil. student supervised by Cas Cremers at the University of Oxford, and not worrying about the Internet, which he now studies whenever he can.

MARK M. WILDE was born in Metairie, Louisiana, USA. He received the Ph. D. in electrical engineering from the University of Southern California, Los Angeles, in 2008, and was advised by Todd Brun. He is an Assistant Professor in the Department of Physics and Astronomy and the Center for Computation and Technology at Louisiana State University. His current research interests are in quantum Shannon theory, quantum optical communication, quantum computational complexity theory, and quantum error correction. He has elected not to include any humor in his bio because he finds the above three bios to be about as unfunny as "unfunny" can be and fears that any attempt of his would be worse. He also recognizes that this is the first time he has roasted his coauthors in the second-to-last sentence of a published scientific paper.