A Quasipolynomial-Time Algorithm for the Quantum Separability Problem

Fernando G.S.L. Brandão*  
Universidade Federal de Minas Gerais

Matthias Christandl†  
ETH Zurich

Jon Yard‡  
Los Alamos National Laboratory

ABSTRACT

We present a quasipolynomial-time algorithm for solving the weak membership problem for the convex set of separable, i.e. non-entangled, bipartite density matrices. The algorithm decides whether a density matrix is separable or whether it is ε-away from the set of the separable states in time \( \exp(O(\epsilon^{-2} \log |A| \log |B|)) \), where |A| and |B| are the local dimensions, and the distance is measured with either the Euclidean norm, or with the so-called LOCC norm. The latter is an operationally motivated norm giving the optimal probability of distinguishing two bipartite quantum states, each shared by two parties, using any protocol formed by quantum local operations and classical communication (LOCC) between the parties. We also obtain improved algorithms for optimizing over the set of separable states and for computing the ground-state energy of mean-field Hamiltonians.

The techniques we develop are also applied to quantum Merlin-Arthur games, where we show that multiple provers are not more powerful than a single prover when the verifier is restricted to LOCC protocols, or when the verification procedure is formed by a measurement of small Euclidean norm. This answers a question posed by Aaronson et al. (Theory of Computing 5, 1, 2009) and provides two new characterizations of the complexity class QMA, a quantum analog of NP.

Our algorithm uses semidefinite programming to search for a symmetric extension, as first proposed by Doherty, Parrilo and Spedalieri (Phys. Rev. A, 69, 022308, 2004). The bound on the runtime follows from an improved de Finetti-type bound quantifying the monogamy of quantum entanglement. This result, in turn, follows from a new lower bound on the quantum conditional mutual information and the entanglement measure squashed entanglement.

1. INTRODUCTION

A central problem in quantum information theory is to characterize entanglement in quantum states shared by two or more parties [23]. A bipartite density matrix, or state, is a positive semidefinite matrix \( \rho_{AB} \) on the tensor product \( AB \equiv A \otimes B \) of finite dimensional complex vector spaces that is normalized, meaning \( \text{tr}(\rho_{AB}) = 1 \). Such a state is separable if it can be written as \( \rho_{AB} = \sum_k p_k \rho_{A,k} \otimes \rho_{B,k} \), for local states \( \rho_{A,k} \) and \( \rho_{B,k} \) and probabilities \( p_k \). Any separable state can be created by local quantum operations and classical communication (LOCC) by Alice and Bob and thus only contains classical correlations. Quantum states that are not separable are called entangled. As the normalized Hermitian matrices on \( AB \) form a real vector space of dimension \( d = |A|^2|B|^2 - 1 \) (we abbreviate \( \dim(A) = |A| \)), the set of all states can be viewed as a compact, convex subset of \( \mathbb{R}^d \) containing the convex subset \( S \equiv S_{AB} \) of separable states.

A fundamental question is to decide, given a description of \( \rho_{AB} \) (say, as a rational vector in \( \mathbb{R}^d \)) whether or not it is separable [23] [13] [25] [18] [16] [19], i.e. whether or not it is contained in \( S \). This can be formalized as a decision problem via the weak membership problem. Given a norm \( \| \cdot \| \) on \( \mathbb{R}^d \) and a closed subset \( A \subset S \), let \( \| \rho - A \| = \min_{\sigma \in A} \| \rho - \sigma \| \) be the distance from \( \rho \) to \( A \).

**Problem 1.** \( W_{SEP}(\epsilon, \| \cdot \|) \) (Weak membership problem for separability): Given a density matrix \( \rho_{AB} \) with the promise that either (i) \( \rho_{AB} \in S \) or (ii) \( \| \rho_{AB} - S \| \geq \epsilon \), decide which is the case.

This problem has been intensely studied in recent years (see e.g. [23] [13] [25] [18] [16] [19]) with the norm given either by the Euclidean norm \( \| X \|_2 \equiv \text{tr}(X^\dagger X)^{1/2} \) or by the trace norm \( \| X \|_1 \equiv \text{tr} \sqrt{X^\dagger X} \).

The best-known algorithms for \( W_{SEP}(\epsilon, \| \cdot \|) \) [13] [25] (with the norm equal either to Euclidean or trace norm) have worst-case complexity \( \exp(O(|A|^2|B|^2 \log(e^{-1})) \)). On the hardness side, Gurvits [18] proved that \( W_{SEP}(\epsilon, \| \cdot \|) \) is...
NP-hard for $\epsilon = \exp(-O(d))$, with $d = \sqrt{|A||B|}$; the dependence on $\epsilon$ was later improved to $\epsilon = 1/\poly(d)$ [16]. The same results apply to the trace norm, since for every $l \times l$ matrix, $||X||_l \geq ||X||_2 \geq l^{-1/2}||X||_1$.

A second problem closely related to the weak-membership problem for separability is the following:

**Problem 2. BSS(ε) (Best Separable State):** Given a Hermitian matrix $M$ on $AB$, estimate $\max_{\sigma \in S} \tr(M\sigma)$ with additive error $\epsilon$.

The BSS(ε) problem thus consists of optimizing a linear function over the convex set of separable states $S$. It is a standard fact in convex optimization [17] that linear optimization and weak-membership over a convex set are equivalent tasks, which implies that BSS(ε) can be used to solve $W_{\SEP}(\delta, \|\cdot\|)$ and vice-versa, up to a poly($d$) loss in the error parameters $\epsilon$ and $\delta$ (see [24] for a detailed analysis). The best known algorithm for BSS(ε) has worst-case complexity $O(\epsilon^{-2}\|A\|\log(\epsilon^{-1}))$ [1]. The NP-hardness of the weak-membership problem for separability implies that BSS(ε) is NP-hard for $\epsilon = 1/\poly(d)$. Conditioned on the stronger assumption that there is no subexponential-time algorithm for 3-SAT [24], Harrow and Montanaro [19], building on work by Aaronson et al. [1], recently ruled out even quasipolynomial-time algorithms for BSS(ε) of complexity up to $O(\epsilon^{-2}\|A\|\log(\epsilon^{-1})\|M\|_\infty)$ for constant $\epsilon$ and any $\nu + \mu > 0$. More specifically, they showed one could solve 3-SAT with $n$ clauses by solving BSS(ε), with constant $\epsilon$, for a matrix $0 \leq M \leq I$ on $AB$ with $|A| = |B| = 2^{O(\sqrt{\nu}\polylog(n))}$. Indeed, this shows that an algorithm for BSS(ε) with time complexity $O(\epsilon^{-2}\|A\|\log(\epsilon^{-1})\|M\|_\infty)$ would imply an $O(n^{1-(\nu+\mu)/2}\polylog(n))$-time algorithm for 3-SAT.

The best separable state problem has a number of other applications (see e.g. [19]), including the estimation of the ground-state energy of mean-field quantum Hamiltonians and estimating the minimal min-entropy of quantum channels. In entanglement theory, it has been studied under the name of optimization of entanglement witnesses (see e.g. [24]).

It turns out that the problem BSS(ε) is also intimately connected to quantum Merlin-Arthur games with multiple Merlins. The class QMA is a quantum analog of NP and is formed by all languages that can be decided in quantum polynomial-time by a verifier who is given a quantum system of polynomially many qubits as a proof (see e.g. [13]). The class QMA(2), in turn, is a variant of QMA in which two proofs, not entangled with one another, are given to the verifier [27]. The properties of QMA(2) and its relation to QMA have recently been in the center of interest in quantum complexity theory [10, 27, 11, 13, 5, 28, 2]. As shown in [10], the optimal acceptance probability of a QMA(2) protocol can be expressed as a BSS(ε) instance. Thus a better understanding of the latter would also shed light on the properties of QMA(2).

2. RESULTS

A quasipolynomial-time algorithm for separability: Our main result is a quasipolynomial-time algorithm for $W_{\SEP}(\epsilon, \|\cdot\|)$, for two different choices of the norm:

**Theorem 1.** $W_{\SEP}(\epsilon, \|\cdot\|_2)$ and $W_{\SEP}(\epsilon, \|\cdot\|_{\text{LOCC}})$ can be solved in $O(\epsilon^{-2}\log|A|\log|B|)$ time.

The norm $\|\cdot\|_{\text{LOCC}}$ can be seen as a restricted version of the trace norm $\|\cdot\|_1$. The latter can be written as $||X||_1 = \max_{0 \leq M \leq 1} \tr((2M - I)X)$, where $I$ is the identity matrix, and is of special importance in quantum information theory as it is directly related to the optimal probability for distinguishing two equiprobable states $\rho$ and $\sigma$ with a quantum measurement [4]. In analogy with this interpretation of the trace norm, we define the LOCC norm as [30]:

$$||X||_{\text{LOCC}} := \max_{M \in \text{LOCC}} \tr((2M - I)X),$$

where LOCC is the convex set of matrices $0 \leq M \leq I$ such that there is a two-outcome measurement $\{M, I - M\}$ that can be realized by LOCC [5].

The optimal bias in distinguishing $\rho$ and $\sigma$ by any LOCC protocol is then $\frac{1}{2}||\rho - \sigma||_{\text{LOCC}}$. We note that in many applications of the separability problem, e.g. assessing the usefulness of a quantum state for violating Bell's inequalities or for performing quantum teleportation, the LOCC norm is actually the more relevant quantity to consider.

The Euclidean, or Frobenius norm $||X||_F := \tr(X^\dagger X)$ is the negative exponential of the quantum collision entropy, and is often of interest in quantum information theory because its quadratic nature makes it especially easy to work with.

The algorithm for testing separability, which we present and analyze in more detail in Section 3, is very simple and works by verifying the existence of a quantum state with a property that distinguishes two states $\rho$ and $\sigma$ (see e.g. [19]).

A quasipolynomial-time algorithm for Best Separable State: The same method used to prove Theorem 1 also results in the following new algorithm for BSS(ε):

$\|M\|_\infty$ is the operator norm of $M$, given by the maximum eigenvalue of $\sqrt{M^*M}$.

$\|\cdot\|_{\text{LOCC}}$ is a quantified norm that has been in the center of interest in quantum complexity theory [10, 27, 11, 13, 5, 28, 2].

$\|\cdot\|_{\text{LOCC}}$ is the norm that is formed by all languages that can be decided in quantum complexity theory [10, 27, 11, 13, 5, 28, 2].

$\|\cdot\|_{\text{LOCC}}$ is a quantified norm that has been in the center of interest in quantum complexity theory [10, 27, 11, 13, 5, 28, 2].
THEOREM 2. There is an algorithm solving BSS(ε) for the Hermitian operator \( M \) in time
\[
\exp\left( O\left( \frac{1}{2} \log|A| \log|B| \frac{1}{|M|} \right) \right).
\]

Furthermore, there is an \( \exp\left( O\left( \frac{1}{2} \log|A| \log|B| \right) \right) \) -time algorithm solving BSS(ε) for any \( M \) such that \( \{M, I - M\} \) is an LOCC measurement.

It is intriguing that the complexity of our algorithm for LOCC operators \( M \) matches the hardness result of Harrow and Montanaro for general operators, which shows that a subexponential-time algorithm of complexity up to
\[
\exp\left( O\left( \frac{1}{2} \log|A| \log|B| \frac{1}{|M|} \right) \right)
\]
for constant \( \varepsilon \) and any \( \nu + \mu > 0 \) would imply a \( \exp(o(n)) \) algorithm for SAT with \( n \) clauses. It is an open question if a similar hardness result could be obtained for LOCC measurements, which would imply that our algorithm is optimal, assuming SAT requires exponential time.

An application of Theorem 2 concerns the estimation of the ground state energy of mean-field Hamiltonians. A mean-field Hamiltonian consists of a Hermitian operator acting on \( n \) sites (each formed by a \( d \)-dimensional quantum system) defined as \( H := \frac{1}{n} \sum_{i,j} K_{ij} \), with \( K_{ij} \) given by the Hermitian matrix which acts as \( K \) on sites \( i \) and \( j \) (for a fixed two-sites interaction \( K \)) and as the identity on the remaining sites. Mean-field Hamiltonians are often used in condensed-matter physics as a substitute for a given local Hamiltonian, since they are easier to analyze and in many cases provide a good approximation to the true model.

An important property of quantum many-body Hamiltonians is their ground-state energy, i.e. their minimal eigenvalue. A folklore result in condensed-matter physics, formalized e.g. in [13], is that the computation of the ground-state energy of a mean-field Hamiltonian \( H \) is equivalent to the minimization of \( \text{tr}(\sigma K) \) over separable states \( \sigma \in S_{A,B} \) with \( |A| = |B| = d \). Theorem 2 then readily implies an \( \exp\left( O\left( \frac{1}{2} \log^2(d)|K|_2^2 \right) \right) \) -time algorithm for the problem. Before, the best-known algorithm [5] scaled as
\[
\exp\left( \Omega\left( d|K|_\infty \log(1/d) \right) \right).
\]

Monogamy of entanglement and LOCC norm:
We say that a bipartite state \( \rho_{A:B} \) is k-extendible if there is a state \( \rho_{A:B_1,\ldots,B_k} \) that is permutation-symmetric in the \( B \) systems with \( \rho_{A:B} = \text{tr}_{B_2,\ldots,B_k}(\rho_{A:B_1,\ldots,B_k}) \). The sets of k-extendible states provide a sequence of approximations to the set of separable states. In the limit of large \( k \), the approximation becomes exact because a state is separable if, and only if, it is k-extendible for every \( k \) (see e.g. [9]). This result is a manifestation of a property of quantum correlations known as monogamy of entanglement: a quantum system cannot be equally entangled with an arbitrary number of other systems, i.e. entanglement is a non-shareable property of quantum states.

In a quantitative manner, quantum versions of the de Finetti theorem imply that for any k-extendible state \( \rho_{A:B} \):
\[
\|\rho_{A:B} - S\|_1 \leq 4|B|k^{-1} \varepsilon.\]
Moreover, this bound is close to tight, as there are k-extendible states that are \( \Omega(|B|k^{-1}) \) -away from the set of separable states [2]. Unfortunately, for many applications this error estimate – exponentially large in the number of qubits of the state – is too big to be useful. The key result behind Theorems 1 and 2 is the following de Finetti-type result, which shows that a significant improvement is possible if we are willing to relax our notion of distance of two quantum states:

THEOREM 3. Let \( \rho_{A:B} \) be k-extendible. Then
\[
\|\rho_{A:B} - S\|_{\text{LOCC}} \leq O(k^{-1} \log|A|)^{\frac{1}{2}}.
\]

In [30] it was shown that \( \|X\|_{\text{LOCC}} \geq \frac{1}{\sqrt{\text{dim}}(X)} \|X\|_2 \), so we also have a similar bound for the Euclidean norm, namely
\[
\|\rho_{A:B} - S\|_2 \leq O(k^{-1} \log|A|)^{\frac{1}{2}}\]

A direct implication of Theorem 3 concerns data-hiding states [12, 11, 14, 21]. Every state \( \rho \) that can be well-distinguished from separable states by a global measurement, yet is almost completely indistinguishable from a separable state by LOCC measurements is a so-called data-hiding state: it can be used to hide a bit of information (whether the prepared state is \( \rho \) or the closest separable state to \( \rho \) in LOCC norm) that is not accessible by LOCC operations alone. The bipartite antisymmetric state of sufficiently high dimension is an example of a data hiding state [13], as are random mixed states with high probability [21] (given an appropriate choice of the dimensions and the rank of the state). Theorem 3 shows that highly extendible states that are far away in trace norm from the set of separable states must necessarily be data-hiding.

Quantum Merlin-Arthur games with multiple Merlins: A final application of Theorem 3 concerns the complexity class Quantum Merlin-Arthur (QMA), the quantum analogue of NP (or more precisely of MA). It is natural to ask how robust the definition of QMA is and a few results are known in this direction: For example, it is possible to amplify the soundness and completeness parameters to exponential accuracy, even without enlarging the proof size [23]. Also, the class does not change if we allow a first round of logarithmic-sized quantum communication from the verifier to the prover [3].

From Theorem 2 we get a new characterization of QMA, which at first sight might appear to be strictly more powerful: We show QMA to be equal to the class of languages that can be decided in polynomial time by a verifier who is given \( k \) unentangled proofs and can measure them using any quantum polynomial-time implementable LOCC protocol among the \( k \) proofs. This answers an open question of Aaronson et al. [1]. We hope this characterization of QMA proves useful in devising new QMA verifying systems.

In order to formalize our result, let \( M \) be a class of two-outcome measurements and consider the classes QMA\(_{(k)_{m,s,c}}\), defined in analogy to QMA as follows [27, 19]:

\[\text{In fact, the operator } M \text{ can be taken to be a non-normalized separable state [19]. This, however, does not imply that it can be implemented by LOCC.}\]

\[\text{The algorithm again simply searches for the minimum overlap of } K \text{ over an } \epsilon \text{-net in the set of product states.}\]
Definition 1. A language $L$ is in $\text{QMA}_m(k)_{m,s,c}$ if there is a uniform family of polynomial-sized quantum circuits that, for every input $x \in \{0,1\}^n$, can implement a two-outcome measurement $\{M_x, I-M_x\}$ from the class $M$ such that

- Completeness: If $x \in L$, there exist $k$ witnesses $|\psi_1\rangle, \ldots, |\psi_k\rangle$, each of $m$ qubits, such that
  $$\text{tr} (M_x (|\psi_1\rangle \langle \psi_1| \otimes \cdots \otimes |\psi_k\rangle \langle \psi_k|)) \geq c.$$

- Soundness: If $x \not\in L$, then for any states $|\psi_1\rangle, \ldots, |\psi_k\rangle$
  $$\text{tr} (M_x (|\psi_1\rangle \langle \psi_1| \otimes \cdots \otimes |\psi_k\rangle \langle \psi_k|)) \leq s.$$

We call $\text{QMA}_m(k)$ $\text{QMA}_m(k)_{\text{poly}(n),2,3,1/3}$. By a uniform family, we mean that there should be a classical algorithm which, upon given the input length $n$ and the string $x$, outputs a description of the quantum circuit implementing the measurement $\{M_x, I-M_x\}$ in time $O(\text{poly}(n))$.

Let $\text{SEP}_{YES}$ be the class of two output POVMs $\{M, I-M\}$ such that $M$, the POVM element corresponding to accept, is a (non-normalized) separable operator. Harrow and Montanaro showed that

$$\text{QMA}_{\text{SEP}_{YES}}(2) = \text{QMA}(2) = \text{QMA}(k)$$

for any $k = \text{poly}(n)$ [19], i.e. two proofs are just as powerful as $k$ proofs and one can restrict the verifier’s action to $\text{SEP}_{YES}$ without changing the expressive power of the class.

We define $\text{QMA}_{\text{LOC}}(k)$ in an analogous way, but now the verifier can only measure the $k$ proofs with a LOCC measurement. Then we have,

Theorem 4. For $k = O(1)$,

$$\text{QMA}_{\text{LOCC}}(k) = \text{QMA}.$$  \hspace{1cm} (2)

In particular,

$$\text{QMA}_{\text{LOC}}(k)_{m,s,c} \subseteq \text{QMA}_{\text{O}(m^{2^{-\epsilon}}, s, s+c, c)}.$$

A preliminary step in the direction of Theorem 4 is the following [3], where a similar result was shown for $\text{QMA}_{\text{LOC}}(k)$, a variant of $\text{QMA}(k)$ in which the verifier is restricted to implement only local measurements on the $k$ proofs and jointly post-process the outcomes classically.

It is an open question whether Eq. (2) remains true if we consider $\text{QMA}(2)$ instead of $\text{QMA}_{\text{LOC}}(2)$. If this turns out to be the case, then it would imply an optimal conversion of $\text{QMA}(2)$ into $\text{QMA}$ in what concerns the proof length (under a plausible complexity-theoretic assumption). For it follows from [19] (based on the $\text{QMA}(\sqrt{n} \text{poly}(n))_{\log(n),1/3,1}$ protocol for $3$-SAT with $n$ variables of [1]) that unless there is a subexponential-time quantum algorithm for $3$-SAT, then there is a constant $\epsilon_0 > 0$ such that for every $\delta > 0$,$^{10}$

$$\text{QMA}(2)_{m,s,c} \not\subseteq \text{QMA}(\text{O}(m^{2^{-\delta}}, s, s+c, c))$$

Recently Chen and Drucker [8] showed that a variant of the $3$-SAT protocol from [1] can be implemented with only local measurements, showing that $3$-SAT is in

$$\text{QMA}_{\text{LOC}}(\sqrt{n} \text{poly}(n))_{\log(n),1/3,2/3},$$

$^9$\text{QMA}_{\text{LOC}}(k)$ is also called BellQMA(k) [1] since the verifier is basically restricted to perform a Bell test on the proofs.

$^{10}$In fact they proved the stronger statement that $3$-SAT is in $\text{QMA}_{\text{LOC}}(\sqrt{n} \text{poly}(n))_{\log(n),1/3,2/3}$. It is an intriguing open question if one could also obtain a $\text{QMA}_{\text{LOC}}(2)$ protocol with the same total proof length ($O(\sqrt{n} \text{poly}(n))$), which would imply that the reduction from $\text{QMA}_{\text{LOC}}(2)$ to $\text{QMA}$ given in Theorem 4 cannot be improved, unless there is a subexponential time quantum algorithm for SAT.

We will now give a characterization of $\text{QMA}$ in terms of protocols for multiple provers with a restriction on the Euclidean norm of the verifiers’ measurements. Let $\text{QMA}_{\text{LOW},c}(k)$ be defined as above, with $\text{LOW}$ the class of measurements $\{M, I-M\}$ for which $\|M\|_2 \leq \text{poly}(n)$, but with such a restriction imposed only on the no instances of the language.

Definition 2. A language $L$ belongs to $\text{QMA}_{\text{LOW},c}(k)$ if there is a uniform family of quantum circuits that, for every $x \in \{0,1\}^n$, can implement a two-outcome measurement $\{M_x, I-M_x\}$ such that

- Completeness: If $x \in L$, there exist $k$ witnesses $|\psi_1\rangle, \ldots, |\psi_k\rangle$, each of $\text{poly}(n)$ qubits, such that
  $$\text{tr} (M_x (|\psi_1\rangle \langle \psi_1| \otimes \cdots \otimes |\psi_k\rangle \langle \psi_k|)) \geq \frac{2}{3}.$$  

- Soundness: If $x \not\in L$, then $\|M_x\|_2 \leq \text{poly}(n)$ and for any $|\psi_1\rangle, \ldots, |\psi_k\rangle$
  $$\text{tr} (M_x (|\psi_1\rangle \langle \psi_1| \otimes \cdots \otimes |\psi_k\rangle \langle \psi_k|)) \leq \frac{1}{3}.$$

Then we also have

Theorem 5. For $k = O(1)$,

$$\text{QMA}_{\text{LOW},c}(k) = \text{QMA}.$$
Then $\Lambda$ is a $(O(\varepsilon^{-2} \log |A| \log |B|), \varepsilon, 0)$-disentangler in LOCC norm.

**A lower bound on conditional mutual information:**
The main technical tool we use for obtaining Theorem 3 is a new lower bound on the quantum conditional mutual information of tripartite quantum states $\rho_{ABE}$, which might be of independent interest. The conditional mutual information is defined as

$$I(A;B|E)_{\rho} := H(A|E)_{\rho} + H(B|E)_{\rho} - H(A,B|E)_{\rho} - H(E)_{\rho},$$

where $H(X)_{\rho} := -\operatorname{tr}(\rho_X \log \rho_X)$ is the von Neumann entropy. Then we have the following analog of Pinsker’s inequality of the algorithm solving the SDP is good enough, which we now analyze in detail.

Consider the following semidefinite program, with $\tau_{AB} = 1/(|A||B|)$ the maximally mixed state, $\delta := \varepsilon/2$ and $\rho_{AB,\delta} := (1-\delta)\rho_{AB} + \delta \tau_{AB}$.

$$\max \operatorname{tr}(X_{AB}b_i) \text{ subject to: } X_{AB}b_i \geq 0, X_{AB}b_j \leq \rho_{AB,\delta} \forall j.$$ (4)

We introduced $\rho_{AB,\delta}$ as we require a non-negligible bound on the minimum eigenvalue of the state. Observe that $\rho_{AB,\delta}$ has a $k$-extension precisely when the solution of (4) is 1, in which case the extension is obtained by symmetrizing the $B$ parts of $X$, i.e. by replacing $X$ with the operator

$$\frac{1}{k!} \sum_{\pi \in S_k} (\mathcal{A}_B \otimes \pi_B) X (\mathcal{A}_B \otimes \pi_B)^{-1},$$

where the sum is over all permutations.

We now consider the approximate case. Define

$$\mathcal{F} := \{X_{AB}b_i : X \geq 0, X_{AB}b_i \leq \rho_{AB,\delta} \forall j \in [k]\}$$

as the set of feasible points and $\mathcal{F}_\nu$ its $\nu$-interior, i.e.

$$\mathcal{F}_\nu := \{X_{AB}b_i : X \in \mathcal{F} \text{ for all } H \text{ s.t. } \|H\|_2 \leq \nu\}.$$ 

The use of Frobenius norm in the definition of $\mathcal{F}_\nu$ is completely independent of the norm in the theorem statement. Rather, it ensures the ellipsoid algorithm solves problem (4) up to additive error $\nu$ in time poly($|A||B|^4, \log(1/\nu)$) as long as $\mathcal{F}_\nu$ is nonempty (see e.g. [34] and references therein). We claim that $\mathcal{F}_\nu$ is nonempty when $\nu := \exp(-|A||B|e^{-2})$ and $k = O(\nu^{-1} \log |A|)$. Before proving this, let us show how it implies that we can solve the weak-membership problem for separability by solving (4).

Suppose first that $\rho_{AB}$ is separable. Convexity of $S$ implies that $\rho_{AB,\delta}$ is also separable, so we know there is a symmetric extension $\rho_{A,B_1 \cdots B_k,\delta}$ of $\rho_{AB,\delta}$. The ellipsoid algorithm applied to problem (4) will therefore return a number bigger than $1 - \nu$.

Suppose now that $\rho_{AB} \in S$ away from $S$. Then $\rho_{AB,\delta} \in \varepsilon/2$-away from $S$. By Theorem 3 any state $\rho_{AB}$ that is $\varepsilon/4$-close to $\rho_{A,B_1 \cdots B_k,\delta}$ in LOCC norm does not have a $O(\varepsilon^{-2} \log |A|)$-extension. From this we can get that the solution of the SDP (4) will be smaller than $1 - \Omega(\varepsilon)$. Indeed suppose it were not the case that the solution was larger than $1 - \varepsilon$ (for sufficiently small $\varepsilon > 0$). Then because we are guaranteed to be at most $\nu$ away from the exact solution of (4), this would imply there is a positive semidefinite matrix $Y_{A,B_1 \cdots B_k}$ such that $Y_{A,B_1 \cdots B_k} \leq \rho_{AB,\delta}$ for every $j \in [k]$ and $\operatorname{tr}(Y) \geq 1 - (\varepsilon + \nu)$. We can symmetrize the $B$ systems in $Y_{A,B_1 \cdots B_k}$ to obtain a semidefinite positive matrix $Z_{A,B_1 \cdots B_k}$, symmetric under the exchange of the $B$ systems and such that $Z_{A,B_1 \cdots B_k} \leq \rho_{AB,\delta}$ and $\operatorname{tr}(X) \geq 1 - (\varepsilon + \nu)$. Defining $\sigma_{A,B_1 \cdots B_k} = Z/\operatorname{tr}(Z)$, we find $\sigma_{A,B_1 \cdots B_k}$ to be $k$-extendible with $\sigma_{A,B_1 \cdots B_k} \leq (1 + 2(\varepsilon + \nu))\rho_{AB,\delta}$, so $\|\sigma_{A,B_1 \cdots B_k} - \rho_{AB,\delta}\|_1 \leq 4(\varepsilon + \nu)$. But this is a contradiction, since we found before that the $\varepsilon/4$-ball around $\rho_{AB,\delta}$ does not contain any $k$-extendible state. Because $k = O(\varepsilon^{-2} \log |A|)$, the computational cost of solving the ellipsoid algorithm with accuracy $\nu = \exp(-|A||B|e^{-2})$ is

$$\text{polylog}(1/\nu) \text{ poly}(|A||B|^k) = \exp(O(\varepsilon^{-2} \log |A| \log |B|) + O(\log(|A||B|e^{-1})))$$

$$= \exp(O(\varepsilon^{-2} \log |A| \log |B|)).$$
We now prove that $F_\nu$ is nonempty. This follows from the fact that $T_{A_1 B_1 \cdots B_k} := \frac{1}{\sqrt{2}} T_{A_1 B_1 \cdots B_k} \in F_\nu$, where $T_{A_1 B_1 \cdots B_k} := \mathbb{I}/|A||B|^k$ the maximally mixed state. Indeed, it is clear that $T_{A_1 B_1 \cdots B_k} + H \geq 0$ for every
\[
 ||H||_\infty \leq ||H||_2 \leq \exp(-|A||B|e^{-2}).
\]
Moreover, $T_{A_1 B_1 \cdots B_k} - H \geq 0$ which immediately implies that $tr_{B_2 \cdots B_k}(T + H) \leq tr_{B_2 \cdots B_k}(2T) \leq \rho_{A, B, S}$. □

**Proof of Theorem 2** Let $\mathcal{E}_k$ be the set of $k$-extendible states. Let us first analyze the case in which $M$ is such that $\{M, \mathbb{I} - M\}$ is LOCC. Then the inclusion $S \subset \mathcal{E}_k$ and Theorem 3 give
\[
\max_{\rho \in \mathcal{E}_k} \text{tr}(\rho M) \geq \max_{\sigma \in S} \text{tr}(\sigma M) \geq \max_{\rho \in \mathcal{E}_k} \text{tr}(\rho M) - \sqrt{O(k^{-1} \log |A|)}.
\]
Hence choosing $k = O(e^{-2} \log |A|)$ we can compute an $\varepsilon$-error additive approximation to BSS($\varepsilon$) by solving the semidefinite program given by maximizing $\text{tr}(M \rho)$ over $k$-extendible states, whose time-complexity is $\exp(O(e^{-2} \log |A| |B|))$.

This proves the first part of the theorem.

To obtain the bound for general $M$, note that $||M(\rho - \sigma)|| \leq ||M||_2 ||\rho - \sigma||_2$ by the Cauchy-Schwarz inequality. Therefore
\[
\max_{\rho \in \mathcal{E}_k} \text{tr}(\rho M) \geq \max_{\sigma \in S} \text{tr}(\sigma M) \geq \max_{\rho \in \mathcal{E}_k} \text{tr}(\rho M) - ||M||_2 \sqrt{O(k^{-1} \log |A|)}.
\]
Then choosing $k = O(e^{-2} \log |A||M||_2^2)$ we can obtain an $\varepsilon$-error additive approximation to BSS($\varepsilon$) by solving a SDP of time-complexity $\exp(O(e^{-2} \log |M||\log |A||\log |B|))$. □

**Proof of Theorem 5** We start by proving Eq. 8. Consider a protocol in QMA$_{\text{LOCC}}(2)_{m, s, \varepsilon}$ given by the LOCC measurement $\{M, \mathbb{I} - M\}$. We construct a QMA$_{O(m^2, 0, s, \varepsilon)}$ protocol that can simulate it: The verifier asks for a proof of the form $\psi_A \otimes \sigma_{B_1} \cdots \sigma_{B_k}$ where $|A| = |B_j| = 2^m$ (each register consists of $m$ qubits) and $k = \Omega(m^{-2})$. He then symmetrizes the $B$ systems obtaining the state $\rho_{A, B_1 \cdots B_k}$ and measures $\{M, \mathbb{I} - M\}$ in the subsystems $A B_i$.

Let us analyze the completeness of the protocol. For completeness, the prover can send $\psi_A \otimes \phi_{B_1} \cdots \otimes \phi_{B_k}$ for states $|\psi\rangle, |\phi\rangle$ such that $\text{tr}(|\phi\rangle \langle \phi| \otimes |\psi\rangle \langle \psi| M) \geq c$. Thus the completeness parameter of the QMA protocol is at least $c$.

For soundness, we note that $\|\rho_{A, B_1 - S}\|_{\text{LOCC}} \leq \varepsilon$ by Theorem 3. Thus, $\{M, \mathbb{I} - M\} \subset \text{LOCC}$ the soundness parameter for the QMA protocol can only be $\varepsilon$ away from $s$. Indeed, for every $\rho_{A, B_1 \cdots B_k}$ symmetric in the $B$ systems, $\text{tr}(\rho_{A, B_1} M) \leq \max_{\sigma \in S} \text{tr}(\sigma M) + \|\rho_{A, B_1} - \sigma\|_{\text{LOCC}} \leq s + \varepsilon$.

Eq. (3) follows from the protocol above. Given a protocol in QMA$_{\text{LOCC}}(\ell)$ with each proof of size $m$ qubits we can simulate it in QMA$_{\text{LOCC}}(\ell - 1)$ as follows: The verifier asks for $\ell - 1$ proofs, the first proof consisting of registers $A B_1 \cdots B_k$, each of size $m$ qubits and $k = \Omega(m^{-2})$, and all the $\ell - 2$ other proofs of size $m$ qubits. Then he symmetrizes the $B$ systems and traces out all of them except the first. Finally he applies the original measurement from the QMA$_{\text{LOCC}}(\ell)$ to the resulting state.

The completeness of the protocol is unaffected by the simulation. For the soundness let $\rho_{A_1 \cdots A_k} \otimes \sigma_1 \cdots \sigma_l$ be an arbitrary state sent by the prover (after symmetrizing $B_1, \ldots, B_m$). Let $\{M, \mathbb{I} - M\} \subset \text{LOCC}$ be the verification measurement from the QMA$_{\text{LOCC}}(\ell)$ protocol. Then
\[
\text{tr}(\rho_{A_1 \cdots A_k} \otimes \rho_{\sigma_1} \cdots \otimes \sigma_l M) \leq \max_{\sigma \in S} \text{tr}(\sigma M) + \min_{\sigma \in S} \|\rho_{A_1 \cdots A_k} - \sigma\|_{\text{LOCC}} \leq s + \varepsilon.
\]
The equality in the second line follows since we can assume that the states $\sigma_1, \ldots, \sigma_l$ belong to the verifier and adding local states does not change the minimum LOCC-distance to separable states.

Since for going from QMA$_{\text{LOCC}}(\ell)$ to QMA$_{\text{LOCC}}(\ell - 1)$ we had to blow up one of the proof’s size only by a quadratic factor, we can repeat the same protocol a constant number of times and still get each proof of polynomial size. In the end, the completeness parameter of the QMA procedure is the same as the original one for QMA$_{\text{LOCC}}(\ell)$, while the soundness is smaller than $s + \varepsilon$, which can be taken to be a constant away from $\varepsilon$ by choosing $\varepsilon$ sufficiently small. To reduce the soundness back to the original value $s$ we then use the standard amplification procedure for QMA (see e.g. [33]), which works in this case since the verification measurement is LOCC [1]. □

**Proof of Theorem 11** The proof is very similar to the proof of Theorem 1 so we only comment on the differences. The strategy for simulating a QMA$_{\text{LOCC, na}}(2)$ protocol in QMA is the same as before: The verifier asks for a proof of the form $|\psi\rangle_A \otimes |\phi\rangle_{B_1} \cdots \otimes |\phi\rangle_{B_k}$ where $|A| = |B_j| = 2^m$ (each register consists of $m$ qubits) and $k = \text{poly}(n) e^{-2}$. He then symmetrizes the $B$ systems to obtain the state $\rho_{A, B_1 \cdots B_k}$, and measures $\{M, \mathbb{I} - M\}$ in the subsystems $A B_i$. The completeness of the QMA protocol is the same as that of the original, since the prover can send $|\psi\rangle_A \otimes |\phi\rangle_{B_1} \cdots \otimes |\phi\rangle_{B_k}$.

For analyzing the soundness of the protocol, let $s$ be the closest separable state to $\rho_{A, B_i}$ in Euclidean norm. Eq. (1) gives
\[
\|\rho_{A, B_i} - \sigma\|_2 \leq O(k^{-1} \log |A|)^{1/2} = 1/\text{poly}(n).
\]
Then, by the Cauchy-Schwarz inequality,
\[
\|\text{tr}(\rho_{A, B_i} - \sigma) M_i\|_2 \leq \|\rho_{A, B_i} - \sigma\|_2 \|M_i\|_2 \leq 1/\text{poly}(n).
\]
The proof for QMA$_{\text{LOCC, na}}(k)$ for $k > 2$ is completely analogous to the proof of Theorem 4.

A last point to argue is the converse relation, namely that QMA is contained in QMA$_{\text{LOCC, na}}(2)$. This follows from the QMA error reduction protocol of Marriott and Watrous [20]. Indeed, they showed how any protocol in QMA can be transformed into a protocol with proof size $n$ equal to the original proof size and soundness $2^{-\text{poly}(n)}$. This means that for “no” instances the associated measurement $M_i$ must be such that $\|M_i\|_2 \leq 2^n \|M_i\|_\infty \leq 2^{-\text{poly}(n)}$ from which follows that the protocol is in QMA$_{\text{LOCC, na}}(2)$.
in entanglement theory and is of independent interest. A recursive step (Lemma 3 below) completes the proof. These same lemmas appear in [1] with complete proofs; here we only outline these proofs.

The first step involves an entanglement measure called the regularized relative entropy of entanglement [32], defined as

\[ E_R^\infty(\rho_{AB}) \equiv \lim_{n \to \infty} \frac{1}{n} E_R(\rho_{AB}^\otimes n), \]

where \( E_R(\rho_{AB}) \equiv \min_{\sigma \in S} S(\rho \| \sigma) \) is the relative entropy of entanglement, and where \( S(\rho(\sigma) = \text{tr}(\rho \log \rho - \log \sigma) \) is the quantum relative entropy.

A distinctive property of the relative entropy of entanglement among measurements is the fact that it is not "lockable," meaning that after discarding a small part of the state, \( E_R \) can only drop by an amount proportional to the number of qubits traced out. Indeed, as shown in [22],

\[ E_R(\rho_{ABE}) \leq E_R(\rho_{ABE}) + 2S(B)_\rho. \]

While the same is true for \( E_R^\infty \), we prove the following stronger version:

**Lemma 1.** For every \( \rho_{ABE} \),

\[ I(AB;E) \geq E_R^\infty(\rho_{ABE}) - E_R^\infty(\rho_{AB}). \]

**Proof (outline).** This lemma follows by combining the inequality [1] with an optimal protocol for the following multipartite quantum data compression problem [33]. Consider many copies of a pure state \( |ABEE\rangle \) whose restriction to \( ABE \) is \( \rho_{ABE} \). Suppose these states are shared between two parties: a sender, who holds \( BE \), and a receiver, who holds \( E \), while \( A \) is inaccessible to both. The state redistribution problem asks the sender to use quantum communication [14] to transfer the \( B \) system to the receiver, while asymptotically preserving the overall global quantum state. A protocol for state redistribution was given in [33] achieving the optimal communication rate of \( \frac{1}{2} I(AB;E) \), providing an operational interpretation for quantum conditional mutual information.

The proof of Lemma 1 is obtained by carefully using the state redistribution protocol to apply the inequality [32] to a tensor-power state \( \rho^\otimes n \) in the most efficient way.

Next, we recall a recent operational interpretation of \( E_R^\infty \) in the context of quantum hypothesis testing [7]. Suppose Alice and Bob are given either \( n \) copies of an entangled state \( \rho_{AB} \), or an arbitrary separable state across \( A^n \times B^n \). Then we define \( D_M(\rho_{AB}) \) to be the optimal error exponent for distinguishing between these two situations, using only measurements from the class \( M \). Specifically, let

\[ p_e(n) = \min_{M} \max_{\sigma \in S_{A^nB^n}} \text{tr}(M \sigma), \]

where the minimization is over all measurements \( M \in \mathcal{M} \) identifying \( \rho_{AB}^\otimes n \) with asymptotically unit probability:

\[ \lim_{n \to \infty} \text{tr}(M \rho_{AB}^\otimes n) = 1. \]

A pure state is a rank 1 density matrix. A basic theorem in quantum information asserts that every density matrix \( \rho_A \) can be expressed as the partial trace of a pure state on a larger system \( AB \).

The sender and receiver are also allowed to utilize shared entanglement between themselves to accomplish this task.

The main result of [7] gives the following equality

\[ D_{\text{ALL}}(\rho_{AB}) = E_R^\infty(\rho_{AB}), \]

i.e. the regularized relative entropy of entanglement is the optimal distinguishability rate when trying to distinguish many copies of an entangled state from (arbitrary) separable states, in the case where there is no restrictions on the measurements available.

Define \( \text{LOCC}^- \) in analogy to \( \text{LOCC} \), using only measurements that can be implemented by one-way \( \text{LOCC} \), i.e. by any protocol formed by local operations and classical communication only from Bob to Alice. Then we have:

**Lemma 2.** For every \( \rho_{ABE} \),

\[ E_R^\infty(\rho_{ABE}) - E_R^\infty(\rho_{AB}) \geq D_{\text{LOCC}^-}(\rho_{AB}). \]

**Proof (outline).** The lemma follows by using Eq. [7] and further developing the connection with hypothesis testing in the form of a new monogamy-like inequality for \( E_R^\infty \).

\[ E_R^\infty(\rho_{ABE}) - E_R^\infty(\rho_{AB}) = D_{\text{ALL}}(\rho_{ABE}) - D_{\text{ALL}}(\rho_{AB}) \geq D_{\text{LOCC}^-}(\rho_{AB}). \]

This inequality is proved by using measurements that achieve \( D_{\text{ALL}}(\rho_{AB}) \) and \( D_{\text{LOCC}^-}(\rho_{AB}) \) to construct a global measurement distinguishing \( \rho_{ABE} \) from separable states \( S_{AEB} \) at a sufficiently good rate.

We define in analogy to the \( \text{LOCC} \) norm, the one-way \( \text{LOCC} \) norm \( \| \cdot \|_{\text{LOCC}^-} \), in which only measurements implementable by \( \text{LOCC}^- \) are allowed. Then next step is to convert the entropy bound on \( I(AB;E) \) obtained from Lemmas 1 and 2 into a lower bound in terms of the minimum \( \text{LOCC}^- \) distance to the set of separable states:

**Lemma 3.** For every \( \rho_{AB} \),

\[ D_{\text{LOCC}^-}(\rho_{AB}) \geq \frac{1}{8 \ln 2} \| \rho_{AB} - S_{AB} \|_{\text{LOCC}^-}^2. \]

**Proof (outline).** This follows from a combination of von Neumann's minimax theorem and Azuma's inequality, since separable states satisfy a martingale property when they are subject to local measurements.

So far, Lemmas 1, 2 and 3 combine to give

\[ I(AB;E) \geq E_R^\infty(\rho_{ABE}) - E_R^\infty(\rho_{AB}) \geq D_{\text{LOCC}^-}(\rho_{AB}) \geq \frac{1}{8 \ln 2} \| \rho_{AB} - S_{AB} \|_{\text{LOCC}^-}^2. \]

We now consider the family of norms \( \| \cdot \|_{\text{LOCC}(k)} \), which quantify distinguishability with respect to measurements that can be implemented by \( k \) rounds of \( \text{LOCC} \). In particular, they satisfy \( \text{LOCC}^k = \text{LOCC}(1) \) and \( \text{LOCC} = \cup_k \text{LOCC}(k) \).

Theorem 1 follows by recursive application of the following technical lemma, which is proved in [1]:

**Lemma 4.** Assume that

\[ I(AB;E) \geq \frac{1}{8 \ln 2} \| \rho_{AB} - S_{AB} \|_{\text{LOCC}(k-1)}^2. \]
Then
\[
I(A;B|E) \geq \frac{1}{8 \ln 2} \| \rho_{A:B} - S_{A:B} \|_{\text{LOCC}(k)}^2.
\]

\[\square\]

4. ACKNOWLEDGMENTS

We thank S. Aaronson, M. Berta, A. Harrow, L. Ioannou and A. Winter for helpful discussions. FB and JY thank the Institute Mittag Leffler, where part of this work was done, for their hospitality.

5. REFERENCES

[1] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement. Theory of Computing, 5:1, 2009.
[2] S. Beigi. NP vs QMA_{log}(2). Quantum Inform. Comp., 10:141, 2010.
[3] S. Beigi, P. W. Shor, and J. Watrous. Quantum interactive proofs with short messages. Theory of Computing, 7:201, 2011.
[4] H. Blier and A. Tapp. A quantum characterization of NP. arXiv:0709.0738, 2007.
[5] F. G. S. L. Brandão. Entanglement Theory and the Quantum Simulation of Many-Body Physics. PhD thesis, Imperial College, 2008.
[6] F. G. S. L. Brandão, M. Christandl, and J. Yard. Faithful squashed entanglement. to appear in Comm. Math. Phys., 2011. arXiv:1010.1750.
[7] F. G. S. L. Brandão and M. B. Plenio. A generalization of quantum Stein’s lemma. Comm. Math. Phys., 295:791, 2010.
[8] J. Chen and A. Drucker. Short multi-prover quantum proofs for SAT without entangled measurements. arXiv:1011.0716, 2010.
[9] M. Christandl, R. Koenig, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. Comm. Math. Phys., 273:473, 2007.
[10] M. Christandl and A. Winter. “Squashed entanglement” - an additive entanglement measure. J. Math. Phys., 45:829, 2004.
[11] D. P. DiVincenzo, P. Hayden, and B. M. Terhal. Hiding quantum data. Found. Phys., 33:1629, 2003.
[12] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. IEEE Trans. Inform. Theory, 48:580, 2002.
[13] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. A complete family of separability criteria. Phys. Rev. A, 69:022308, 2004.
[14] T. Egging and R. F. Werner. Hiding classical data in multi-partite quantum states. Phys. Rev. Lett., 89:097905, 2002.
[15] M. Fannes and C. Vandenplas. Finite size mean-field models. J. Phys. A: Math. Gen., 39:13843, 2006.
[16] S. Gharibian. Strong NP-hardness of the quantum separability problem. Quant. Inform. Comp., 10:343, 2010.
[17] M. Grötschel, L. Lovász, and A. Schrijver. Geometric algorithms and combinatorial optimization. Springer-Verlag, 1993.
[18] L. Gurvits. Classical complexity and quantum entanglement. J. Comp. Sys. Sci., 69:448, 2004.
[19] A. Harrow and A. Montanaro. An efficient test for product states, with applications to quantum Merlin-Arthur games. Proc. Found. Comp. Sci. (FOCS), page 633, 2010.
[20] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. Comm. Math. Phys., 250:371, 2004.
[21] P. Hayden, D. Leung, and A. Winter. Aspects of generic entanglement. Comm. Math. Phys., 265:95, 2006.
[22] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Locking entanglement measures with a single qubit. Phys. Rev. Lett., 94(200501), 2005.
[23] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. Rev. Mod. Phys., 81:865, 2009.
[24] R. Impagliazzo and R. Paturi. On the complexity of k-SAT. J. Comp. Sys. Sci., 62(367), 2001.
[25] L. M. Ioannou. Computational complexity of the quantum separability problem. Quant. Inform. Comp., 7:335, 2007.
[26] M. Kowalski and A. Winter. Monogamy of entanglement and other correlations. Phys. Rev. A, 69:022309, 2004.
[27] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In Lecture Notes in Computer Science, volume 2006, page 189. Springer, 2003.
[28] Y.-K. Liu, M. Christandl, and F. Verstraete. Quantum computational complexity of the n-representability problem: QMA-complete. Phys. Rev. Lett., 98:110503, 2007.
[29] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. Computational Complexity, 14:122, 2005.
[30] W. Matthews, S. Wehner, and A. Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. Comm. Math. Phys., 291, 2009.
[31] L. Vandenberghe and S. Boyd. Semidefinite programming. SIAM Review, 38:49, 1996.
[32] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. Phys. Rev. Lett., 78:2275, 1997.
[33] J. Watrous. Quantum computational complexity. In
    *Encyclopedia of Complexity and System Science*. Springer, 2009.

[34] J. Watrous. Semidefinite programs for
    completely-bounded norms. *Theory of Computing*,
    5:217, 2009.

[35] J. Yard and I. Devetak. Optimal quantum source
    coding with quantum information at the encoder and decoder. *IEEE Trans. Inform. Theory*, 55:5339, 2009.