Schrödinger as a Quantum Programmer: Estimating Entanglement via Steering

Aby Philip[1], Soorya Rethinasamy[1], Vincent Russo[2], and Mark M. Wilde[3,1]

[1]School of Applied and Engineering Physics, Cornell University, Ithaca, New York 14850, USA
[2]Unitary Fund
[3]School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA

Quantifying entanglement is an important task by which the resourcefulness of a quantum state can be measured. Here, we develop a quantum algorithm that tests for and quantifies the separability of a general bipartite state by using the quantum steering effect, the latter initially discovered by Schrödinger. Our separability test consists of a distributed quantum computation involving two parties: a computationally limited client, who prepares a purification of the state of interest, and a computationally unbounded server, who tries to steer the reduced systems to a probabilistic ensemble of pure product states. To design a practical algorithm, we replace the role of the server with a combination of parameterized unitary circuits and classical optimization techniques to perform the necessary computation. The result is a variational quantum steering algorithm (VQSA), a modified separability test that is implementable on quantum computers that are available today. We then simulate our VQSA on noisy quantum simulators and find favorable convergence properties on the examples tested. We also develop semidefinite programs, executable on classical computers, that benchmark the results obtained from our VQSA. Thus, our findings provide a meaningful connection between steering, entanglement, quantum algorithms, and quantum computational complexity theory. They also demonstrate the value of a parameterized mid-circuit measurement in a VQSA.

Contents

1 Introduction

Entanglement is a unique feature of quantum mechanics, initially brought to light by Einstein, Podolsky, and Rosen [1]. Many years later, the modern definition of entanglement was given [2], which we recall now. A bipartite quantum state σ_{AB} of two spatially separated systems A and B is separable (unentangled) if it can be written as a probabilistic mixture of product states [2]:

$$\sigma_{AB} = \sum_{x \in \mathcal{X}} p(x)\, \psi_A^x \otimes \phi_B^x, \tag{1}$$

where $\{p(x)\}_{x \in \mathcal{X}}$ is a probability distribution and ψ_A^x and ϕ_B^x are pure states. The idea here is that the correlations between A and B can be fully attributed to a classical, inaccessible random variable with probability distribution $\{p(x)\}_{x \in \mathcal{X}}$.

The definition above is straightforward to write down, but it is a different matter to formulate an algorithm to decide if a general state is separable; in fact, it has been proven to be computationally difficult in a variety of frameworks [3, 4, 5, 6, 7]. Intuitively, deciding the answer requires performing a search over all possible probabilistic decompositions of the state, and there are too many possibilities to consider. Regardless, determining whether a general state ρ_{AB} is separable or entangled, known as the separability problem, is a fundamental problem of interest relevant to various fields of physics, including condensed matter [8, 9, 10], quantum gravity [11, 12, 13, 14, 15], quantum optics [16], and quantum key distribution [17, 18]. In quantum information science, entanglement is the core resource in several basic quantum information processing tasks [17, 19, 20], making the separability problem essential in this field as well.

Part of the challenge in using entangled states for various tasks is that they are hard to produce and maintain faithfully on any physical platform. The utility of entangled states drops off dramatically the further they are from being perfectly or maximally entangled. Therefore, assessing the quality of entangled states produced becomes an important task, thus motivating the problem of quantifying entanglement [21, 22, 23, 24], in addition to deciding whether entanglement is present.

To check whether a state is entangled and to quantify its entanglement content experimentally, a rudimentary approach employs state tomography to reconstruct the density matrix and check whether the matrix represents a state that is entangled [25, 26]. However, the computational complexity of this method scales exponentially with the number of qubits, thus prohibiting its use on larger states of interest. With the rapid development of quantum computers of increasing size, it is already infeasible to perform tomography to estimate the density matrices describing the states of these computers. It is even more daunting to address the separability problem using various well-known one-sided entanglement tests [27, 28, 29, 30]. This leaves us to seek out alternative methods for addressing the separability problem, and one forward-thinking direction is to employ a quantum computer to do so [5, 6, 7, 31].

An approach for addressing the separability problem, which we employ here, involves the quantum steering effect, originally discovered by Schrödinger [32, 33]. The idea of steering is that if two distant systems are entangled, distinct probabilistic ensembles of states can be prepared on one system by performing distinct measurements on the other system. To describe this phenomenon more precisely, we can employ some elementary notions from quantum mechanics. Let ψ_{CD} be a pure state of two distant quantum systems C and D, and let $\rho_C = \mathrm{Tr}_D[\psi_{CD}]$ be the reduced state of the system C. Then by performing a measurement on the system D, it is possible to realize a probabilistic ensemble $\{(p(z), \psi_C^z)\}_z$ of pure states on the system C that satisfies $\rho_C = \sum_z p(z)\psi_C^z$. Moreover, for each possible probabilistic decomposition of ρ_C, a measurement acting on D can realize this decomposition. Steering has been a topic of interest in recent years, with applications to quantum key distribution [34, 35], quantum optics [36, 37], and the foundations of quantum mechanics [38, 39].

As suggested above, we can make a non-trivial link between the separability problem and steering, which offers a quantum mechanical method for approaching the former. To see it, recall that a purification of the separable state σ_{AB} in (1) is a pure state φ_{RAB} that satisfies $\mathrm{Tr}_R[\varphi_{RAB}] = \sigma_{AB}$, and consider that one such choice of the state vector $|\varphi\rangle_{RAB}$ in this case is as follows:

$$|\varphi\rangle_{RAB} = \sum_{x \in \mathcal{X}} \sqrt{p(x)}\, |x\rangle_R \otimes |\psi^x\rangle_A \otimes |\phi^x\rangle_B, \tag{2}$$

where $\{|x\rangle_R\}_{x \in \mathcal{X}}$ is an orthonormal basis. Purifications are not unique, but all other purifications of σ_{AB} are related to the one in (2) by the action of a unitary operation on the reference system R [40]. By inspecting (2), we see that the systems A and B can be steered into the probabilistic ensemble $\{(p(x), \psi_A^x \otimes \phi_B^x)\}_{x \in \mathcal{X}}$ of product states by performing the projective measurement $\{|x\rangle\langle x|_R\}_{x \in \mathcal{X}}$ on the reference system R of φ_{RAB}. This leads to an idea for testing separability in the general case. If purification of a general state ρ_{AB} is available and the state ρ_{AB} is indeed separable, then one can a) try to find the unitary that realizes the purification in (2) and b) perform the measurement $\{|x\rangle\langle x|_R\}_{x \in \mathcal{X}}$ on the reference system R. After receiving the outcome x, one can finally test whether the reduced state is a prod-

uct state.

As we will see in more detail later, the basic idea outlined above is at the heart of our method to test whether a state is separable. Additionally, this approach leads to a quantum algorithm and complexity-theoretic statements for quantifying the amount of entanglement in a state. We thus provide a meaningful connection between steering, entanglement, quantum algorithms, and quantum computational complexity theory, which has not been observed hitherto.

In this paper, we expand on the abovementioned idea to develop various separability tests using the quantum steering effect. Our separability test for mixed states consists of a distributed quantum computation involving two parties: a computationally unbounded server, called a prover, which can, in principle, perform any quantum computation imaginable, and a computationally limited client, called a verifier, which can perform time-efficient quantum computations (see Figure 1). We show in Theorems 1 and 2 that the acceptance probabilities of our algorithms, in the ideal case, are directly related to a bonafide entanglement measure, the fidelity of separability. We also employ concepts from quantum computational complexity theory [41, 42] to understand how difficult this test is to perform. Our second contribution results from a modification of our separability test. In an attempt to design a practical algorithm, we replace the prover with a combination of parameterized unitary circuits and classical optimization techniques to perform the necessary computation. This results in a variational quantum steering algorithm (VQSA) that approximates the aforementioned separability test (see Figure 2). The concept of quantum steering is again at the heart of our VQSA, just like the test for separability that it approximates. Interestingly, we prove that the acceptance probability of both tests is related to an entanglement measure called fidelity of separability [22, 23]. We also generalize our separability test and VQSA to the multipartite setting using appropriate definitions of multipartite separability.

Next, we report the results of simulations of the VQSA on a quantum simulator and find that they show favorable convergence properties. In light of the limited scale and error tolerance of near-term quantum computers, we develop semidefinite programs (SDPs) to approximate the fidelity of separability using positive-partial-transpose (PPT) conditions [27, 24] and k-extendibility [29, 30] to benchmark the results obtained from our VQSA. As variational quantum algorithms (VQAs), in general, are prone to encountering barren plateaus [43], we also explore how we can mitigate this issue for our algorithms by making use of the ideas presented in [44].

Our approach is distinct from recent work on quantum algorithms for estimating entanglement. For example, VQAs have been used to address this problem by estimating the Hilbert–Schmidt distance [45], by creating a zero-sum game using parameterized unitary circuits [46], by employing symmetric extendibility tests [31], by estimating logarithmic negativity [47], and using the positive map criterion [47]. VQAs have also been used to estimate the geometric measure of entanglement of multiqubit pure states [48]. The work of [49] is the closest related to ours, but the test used there requires two copies of the state of interest and controlled swap operations, while our VQSA does not require either. In contrast, we introduce a paradigm for VQAs involving parameterized mid-circuit measurements, which is the core of our method for estimating entanglement, and we suspect that this approach will be helpful in future work for a wide variety of VQAs. Furthermore, as we show in Theorems 1 and 2, the acceptance probabilities of our algorithms, in the ideal case, are directly related to a bonafide entanglement measure, the fidelity of separability.

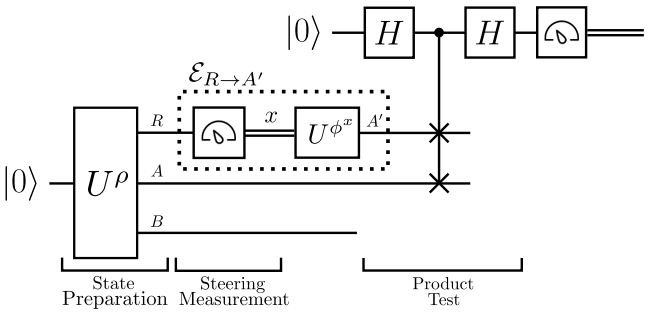


Figure 1: Test for separability of mixed states. The verifier uses a unitary circuit U^ρ to produce the state ψ_{RAB}, which is a purification of ρ_{AB}. The prover (indicated by the dotted box) applies an entanglement-breaking channel $\mathcal{E}_{R\to A'}$ on R by measuring the rank-one POVM $\{\mu_R^x\}_x$ and then, depending on the outcome x, prepares a pure state from the set $\{\phi_{A'}^x\}_x$. The final state is sent to the verifier, who performs a swap test. Theorem 1 states that the maximum acceptance probability of this interactive proof is equal to $\frac{1}{2}(1+F_s(\rho_{AB}))$, i.e., a simple function of the fidelity of separability.

2 Results

2.1 Quantum Interactive Proof for Fidelity of Separability

We first introduce our test for the separability of mixed states. Recall that a bipartite state is separable or unentangled if it can be written in the form given in (1), where $|\mathcal{X}| \leq \operatorname{rank}(\sigma_{AB})^2$ [2, 50].

Our separability test for mixed states consists of a distributed quantum computation involving a prover

and a verifier. The computation (depicted in Figure 1) begins with the verifier preparing a purification ψ_{RAB} of ρ_{AB}. The verifier sends the system R to a quantum prover, whom, in our model, we restrict to performing entanglement-breaking channels. The prover thus performs an entanglement-breaking channel on the reference system R and sends a system A' to the verifier. An entanglement-breaking channel $\mathcal{E}_{R\to A'}$ can always be written as a measure-and-prepare channel [51], as follows:

$$\mathcal{E}_{R\to A'}(\cdot) = \sum_{x\in\mathcal{X}} \operatorname{Tr}[\mu_R^x(\cdot)]\, \phi_{A'}^x, \tag{3}$$

where $\{\mu_R^x\}_{x\in\mathcal{X}}$ is a rank-one positive operator-valued measure (POVM) and $\{\phi_{A'}^x\}_{x\in\mathcal{X}}$ is a set of pure states. (Due to the above measure-and-prepare decomposition of an entanglement-breaking channel, we can alternatively think of the prover as being split into two provers, a first who is allowed to perform a general quantum operation, followed by the communication of classical data to a second prover, who then is allowed to perform a general operation before communicating quantum data to the verifier. However, we proceed with the single-prover terminology in what follows.) By performing the measurement portion of the entanglement-breaking channel, the prover has, in essence, steered the verifier's systems A and B to a certain probabilistic ensemble of pure states. After steering the verifier's system, the prover sends system A' to the verifier using the preparation portion of the entanglement-breaking channel. The verifier finally performs a swap test on system A and A' and accepts if and only if the measurement outcome of the swap test is zero. The standard model in quantum computational complexity theory [41, 42] is that the prover is always trying to get the verifier to accept the computation: in this scenario, the prover steers the verifier's systems A and B to an ensemble that has maximum overlap with a product-state ensemble and then sends an appropriate state to pass the swap test with the highest probability possible.

The maximum acceptance probability of the distributed quantum computation detailed above is equal to

$$\max_{\mathcal{E}\in \mathrm{EB}_{R\to A'}} \operatorname{Tr}[(\Pi_{A'A}^{\mathrm{sym}} \otimes I_{RB})\, \mathcal{E}_{R\to A'}(\psi_{RAB})], \tag{4}$$

where $\Pi_{A'A}^{\mathrm{sym}}$ is the projector onto the symmetric subspace of the A' and A systems, and $\mathrm{EB}_{R\to A'}$ denotes the set of all entanglement-breaking channels with input system R and output system A'. We find in Theorem 1 below that the maximum acceptance probability in (4) can be expressed as a simple function of the fidelity of separability of ρ_{AB}, the latter defined as [22, 23]

$$F_s(\rho_{AB}) \coloneqq \max_{\sigma_{AB}\in \mathrm{SEP}(A:B)} F(\rho_{AB}, \sigma_{AB}), \tag{5}$$

where $\mathrm{SEP}(A:B)$ denotes the set of separable states shared between Alice and Bob and $F(\rho,\sigma) \coloneqq \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$ is the fidelity of the states ρ and σ [52]. The fidelity of separability is also known as the maximum separable fidelity [5, 6, 7]. With this definition, we state the first key theoretical result of our paper:

Theorem 1 *For a pure state ψ_{RAB}, the following holds*

$$\max_{\mathcal{E}\in \mathrm{EB}_{R\to A'}} \operatorname{Tr}[(\Pi_{A'A}^{\mathrm{sym}} \otimes I_{RB})\, \mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1+F_s(\rho_{AB})}{2}, \tag{6}$$

where $F_s(\rho_{AB})$ is the fidelity of separability of the state $\rho_{AB} = \operatorname{Tr}_R[\psi_{RAB}]$.

See the first part of Section 4 for a brief overview of the proof and Appendix A for a detailed proof. Appendices B and C recall some auxiliary results that support the proof in Appendix A. With this theorem, we have established a separability test for mixed states.

2.2 Variational Quantum Steering Algorithm for Fidelity of Separability

We want to point out two important aspects of our separability test from Section 2.1. First, note that the swap test at the end of the computation essentially leads to a measure of overlap between the state of the verifier's system and the state provided by the prover. The other important point is that, in the real world, no computationally unbounded quantum prover is available to provide the ideal states required for the tests.

Taking both these points into consideration, we modify the computational scenario in Figure 1 to a) measure the necessary overlaps directly and b) make use of quantum variational techniques [53] (parameterized unitary circuits and classical optimization of parameters) to approximate the actions of a computationally unbounded prover. The resulting procedure also tests and quantifies the separability of a given state by estimating its fidelity of separability. This procedure is a different quantum variational technique called a variational quantum steering algorithm (VQSA). As can be seen in Figure 2, quantum steering is at the core of the VQSA via the use of a parameterized mid-circuit measurement.

Our VQSA is structured as follows. Let ρ_{AB} denote the state for which we want to estimate the fidelity of separability, and let ψ_{RAB} be a purification of it, which results from the action of the unitary operator U^ρ on the all-zeros pure state $|0\rangle\langle 0|$. Once we have ψ_{RAB}, we can attempt to access all possible pure-state decompositions $\{(p(x), \psi_{AB}^x)\}_{x\in\mathcal{X}}$ of ρ_{AB} by acting on system R

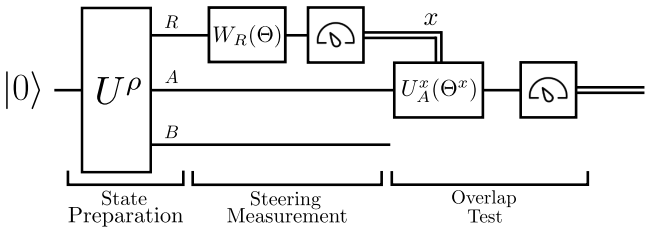


Figure 2: Quantum part of the VQSA to estimate the fidelity of separability $F_s(\rho_{AB})$. The unitary circuit U^ρ prepares the state ψ_{RAB}, which is a purification of ρ_{AB}. The parameterized circuit $W_R(\Theta)$ acts on R to evolve ψ_{RAB} to another purification of ρ_{AB}. The following measurement, labeled "steering measurement," steers the systems AB to be in a pure state ψ_{AB}^x if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuit $U_A^x(\Theta^x)$ and the subsequent measurement accepts with a maximum probability of $F_s(\rho_{AB})$.

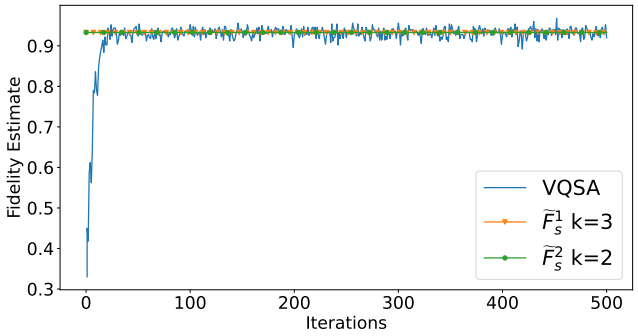


Figure 3: Fidelity of separability calculated for a (3/4,1/4) classical mixture of $|\Phi^+\rangle$ and $|\Phi^-\rangle$ using our VQSA (blue line). The algorithm converges to 0.93, which agrees with the value obtained using the benchmarks $\widetilde{F}_s^1$ and $\widetilde{F}_s^2$.

with unitary operations. We use the first parameterized unitary $W_R(\Theta)$ to do so. To ensure that we have a sufficient number of measurement outcomes (to cover the possible case when $|\mathcal{X}| = \text{rank}(\rho_{AB})^2$), we can prepare some ancilla qubits in the all-zeros state, for a system R', and act with W on R and R'. However, without loss of generality, these extra qubits can be grouped as part of an overall reference system, relabeled as R.

After the action of $W_R(\Theta)$, the reference system is measured in the standard basis, and based on the outcome x, the post-measurement state of the system AB is a pure state ψ_{AB}^x. We then estimate the maximum eigenvalue of the reduced state ψ_A^x: this can be accomplished by performing a parameterized unitary $U_A^x(\Theta^x)$, based on the outcome x, on the reduced state ψ_A^x, measuring all qubits of A in the computational basis, and accepting if the all-zeros outcome occurs.

Using a hybrid quantum-classical optimization loop, we can maximize the acceptance probability to estimate the value of the fidelity of separability. The quantum part of this VQSA is summarized in Figure 2.

Theorem 2 *If the parameterized unitary circuits involved in the quantum part of the VQSA, summarized in Figure 2, can express all possible unitary operators of their respective systems, then the maximum acceptance probability of the quantum circuit is equal to* $F_s(\rho_{AB})$.

See Appendix D for a detailed proof.

2.3 Benchmarking Semidefinite Programs and Examples

Since our algorithms will be running on near-term quantum computers with limited scale and error tolerance, we develop semidefinite programs (SDPs) to benchmark the results from our VQSA because the ideal outcomes can be estimated classically for small numbers of qubits. Our benchmarks $\widetilde{F}_s^1(\rho_{AB}, k)$ and $\widetilde{F}_s^2(\rho_{AB}, k)$ are based on the positive partial transpose (PPT) and k-extendibility hierarchy. See details in Appendices E and F.

We now present an example simulation of our VQSA to demonstrate that it can estimate the fidelity of separability. For our first example, we take the state of interest ρ_{AB} to be a (3/4,1/4) probabilistic mixture of two maximally entangled states, $|\Phi^+\rangle = \sqrt{1/2}(|00\rangle + |11\rangle)$ and $|\Phi^-\rangle = \sqrt{1/2}(|00\rangle - |11\rangle)$, so that

$$\rho_{AB} = \frac{3}{4}|\Phi^+\rangle\langle\Phi^+| + \frac{1}{4}|\Phi^-\rangle\langle\Phi^-|. \tag{7}$$

Systems R, A, and B of the purification of ρ_{AB} contain one qubit each. See Figure 3 for the results. We use the benchmarks and VQSA to estimate the fidelity of separability as ≈ 0.93. We evaluate these benchmarks for different levels of the k-extendibility hierarchy. See Appendix G for more examples and Appendix H for details about the code we developed.

As a second example, we consider a state consisting of four qubits. Let us consider the four qubit state $|\psi\rangle$ defined as follows:

$$\frac{1}{\sqrt{2}}\left(|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{B_1}|0\rangle_{B_2} + |1\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{B_1}|1\rangle_{B_2}\right), \tag{8}$$

where A consists of two qubits A_1 and A_2 and B consists of two qubits B_1 and B_2. We then pass A_1 and A_2 through a qubit depolarizing channel defined as $\mathcal{D}_p(\rho) := (1-p)\rho + p\mathbb{I}/2$ where $p = 0.7$. So, the final state under consideration can be written as

$$\tilde{\rho}_{AB} := \left(\mathcal{D}_{p,A_1} \otimes \mathcal{D}_{p,A_2} \otimes \mathbb{I}_{B_1} \otimes \mathbb{I}_{B_2}\right)\left(|\psi\rangle\langle\psi|\right). \tag{9}$$

We can then use our VQSA to estimate the fidelity of

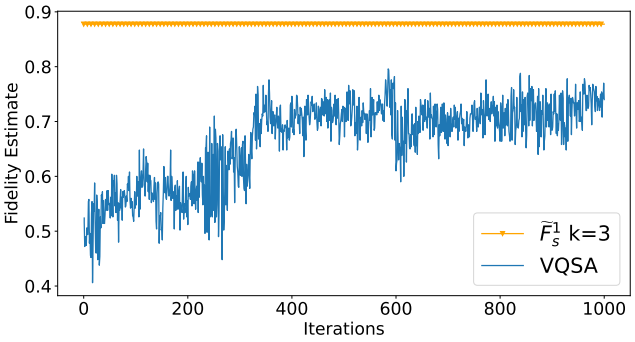


Figure 4: Fidelity of separability calculated for the state $\tilde{\rho}_{AB}$ as specified in (9) using our VQSA (blue line) and $\widetilde{F}_s^1$ (orange line).

separability for $\tilde{\rho}_{AB}$ and compare the result against the previous SDP benchmarks. See Figure 4 for the results.

2.4 Generalization to Multipartite Fidelity of Separability

We also generalize our VQSA to measure the fidelity of separability of multipartite states in the following fashion. A multipartite state $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M}) \equiv \mathcal{D}(\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_M})$ is separable if it can be written as

$$\rho_{A_1\cdots A_M} = \sum_{x\in\mathcal{X}} p(x)\psi_{A_1}^{x,1} \otimes \cdots \otimes \psi_{A_M}^{x,M} \tag{10}$$

where $\psi_{A_i}^{x,i}$ is a pure state for every $x \in \mathcal{X}$ and $i \in \{1,\ldots,M\}$. Let M-SEP denote the set of all $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M})$ such that $\rho_{A_1\cdots A_M}$ is separable.

For the multipartite case of the distributed quantum computation, the verifier prepares a purification $\psi^{\rho}_{RA_1\cdots A_M}$ of $\rho_{A_1\cdots A_M}$. The prover applies a multipartite entanglement-breaking channel on R, which can be written as:

$$\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\cdot) = \sum_{x\in\mathcal{X}} \operatorname{Tr}[\mu_R^x(\cdot)]\left(\phi_{A_1'}^{x,1} \otimes \cdots \otimes \phi_{A_{M-1}'}^{x,M-1}\right), \tag{11}$$

where $\{\mu_R^x\}_x$ is a rank-one POVM and $\{\phi_{A_i'}^{x,i}\}_{x,i}$ is a set of pure states. The prover sends systems $(A^{M-1})' \equiv A_1'\cdots A_{M-1}'$ to the verifier. Finally, the verifier performs a collective swap test on these systems and the systems $A_1\cdots A_M$, as depicted in Figure 5. The acceptance probability of this distributed quantum computation is given by

$$\max_{\mathcal{E}\in \mathrm{EB}_{M-1}} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'A^{M-1}} \mathcal{E}_{R\to(A^{M-1})'}(\psi_{RA^{M-1}})], \tag{12}$$

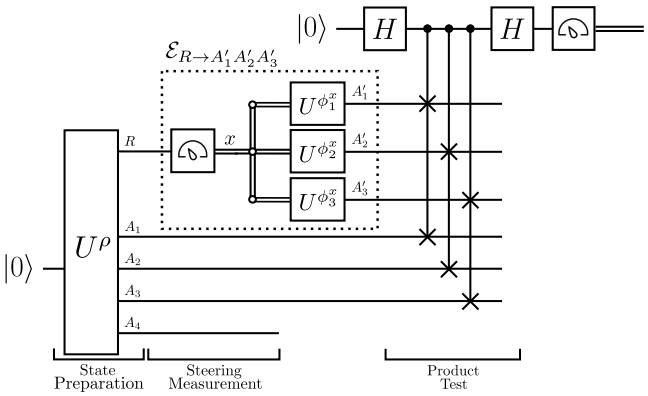


Figure 5: Test for separability of multipartite mixed states. The verifier uses the unitary circuit U^{ρ} to prepare the state $\psi_{RA_1A_2A_3A_4}$, which is a purification of $\rho_{A_1A_2A_3A_4}$. The prover (indicated by the dotted box) applies an entanglement-breaking channel $\mathcal{E}_{R\to A_1'A_2'A_3'}$ on R by measuring the rank-one POVM $\{\mu_R^x\}_{x\in\mathcal{X}}$ and then, depending on the outcome x, prepares a state from the set $\{\phi_{A_1'}^{x,1} \otimes \phi_{A_2'}^{x,2} \otimes \phi_{A_3'}^{x,3}\}_{x\in\mathcal{X}}$. The final state is sent to the verifier, who performs a collective swap test. Theorem 3 states that the maximum acceptance probability of this interactive proof is equal to $\frac{1}{2}(1 + F_s(\rho_{A_1A_2A_3A_4}))$, i.e., a simple function of the fidelity of separability.

where $\Pi^{\mathrm{sym}}_{(A^{M-1})'A^{M-1}}$ is the projection onto the symmetric subspace of systems $(A^{M-1})'$ and A^{M-1} and EB_{M-1} denotes the set of multipartite entanglement-breaking channels defined in (11). This leads to the following theorem:

Theorem 3 *For a pure state $\psi_{RA^M} \equiv \psi_{RA_1\cdots A_M}$, the following equality holds:*

$$\max_{\mathcal{E}\in \mathrm{EB}_{M-1}} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'(A^{M-1})} \mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA^M})] = \frac{1}{2}\left(1 + F_s(\rho_{A_1\cdots A_M})\right), \tag{13}$$

where the multipartite fidelity of separability is defined as

$$F_s(\rho_{A_1\cdots A_M}) \coloneqq \max_{\sigma_{A_1\cdots A_M}\in M\text{-SEP}} F(\rho_{A_1\cdots A_M}, \sigma_{A_1\cdots A_M}). \tag{14}$$

See Appendix I for a proof. We can then use the generalized test of separability of mixed states to develop a VQSA for the multipartite case. See Figure 6. This involves replacing the collective swap test in Figure 5 with an overlap measurement, similar to how we got Figure 2 from Figure 1.

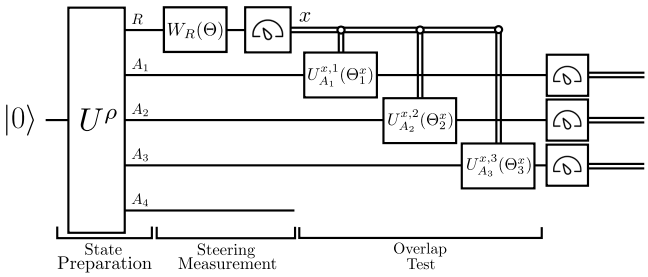


Figure 6: VQSA to estimate the multipartite fidelity of separability $F_s(\rho_{A_1A_2A_3A_4})$. The unitary circuit U^ρ prepares the state $\psi_{RA_1A_2A_3A_4}$, which is a purification of $\rho_{A_1A_2A_3A_4}$. The parameterized circuit $W_R(\Theta)$ acts on R to evolve the state to another purification of $\rho_{A_1A_2A_3A_4}$. The following measurement, labeled "steering measurement," steers the remaining systems to be in a state $\psi^x_{A_1A_2A_3A_4}$ if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuits $U^{x,1}_{A_1}(\Theta^x_1)$, $U^{x,2}_{A_2}(\Theta^x_2)$, and $U^{x,3}_{A_3}(\Theta^x_3)$ are applied and the subsequent measurement accepts with a maximum probability of $F_s(\rho_{A_1A_2A_3A_4})$.

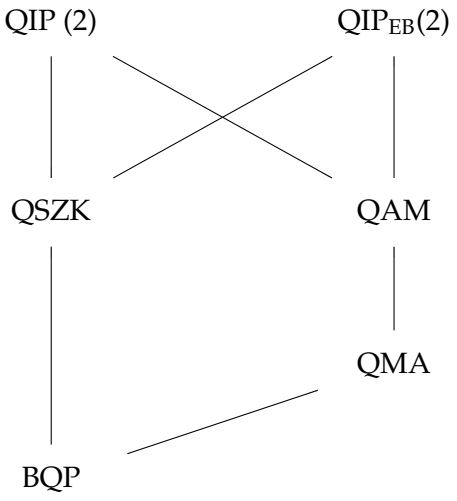


Figure 7: Placement of $\text{QIP}_{\text{EB}}(2)$ relative to other known complexity classes. The complexity classes are organized such that if a class is connected to a class above it, the complexity class placed lower is a subset of the class above. For example, $\text{QIP}_{\text{EB}}(2)$ is a superset of both QSZK and QAM.

2.5 Quantum Computational Complexity Considerations

Our final result is regarding the computational complexity of estimating the fidelity of separability $F_s(\rho_{AB})$. The complexity-theoretic approach allows us to classify the separability problem based on its computational difficulty. Analyses of this form can be effectively conducted within the framework of quantum computational complexity theory [41, 42].

In the paradigm of complexity theory [54], a complexity class is a set of computational problems that require similar resources to solve. If a complexity class A is contained within another class B, then some problems in B could require more computational resources than problems in A. To effectively characterize the difficulty of a class of problems, we pick a problem that is representative of the class or complete for the class. A problem h is considered complete for a complexity class A if h is contained in the class and the ability to solve problem h can be extended efficiently to solve every other problem in A.

To tackle the question posed about the computational complexity of estimating the fidelity of separability, we define $\text{QIP}_{\text{EB}}(2)$ to be the complexity class containing problems that can be solved using a prover restricted to using only entanglement-breaking channels, which processes a quantum message received from the verifier and sends back a quantum message to the verifier. Thus, estimating the fidelity of separability of a given state then falls within $\text{QIP}_{\text{EB}}(2)$, as seen from Figure 1. To fully characterize this novel complexity class, we provide a complete problem for it. We establish that, given quantum circuits to generate a channel $\mathcal{N}_{A\to B}$ and a state ρ_B, estimating the following quantity is complete for $\text{QIP}_{\text{EB}}(2)$:

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\{\varphi^x\}_x,\\ \rho_B=\sum_x p(x)\psi^x_B}} \sum_x p(x)F(\psi^x_B,\mathcal{N}_{A\to B}(\varphi^x_A)). \quad (15)$$

See Appendix J for details and an interpretation of this quantity.

By placing the problem of estimating the fidelity of separability in the class $\text{QIP}_{\text{EB}}(2)$, we establish results that link quantum steering and the separability problem to quantum computational complexity theory. Furthermore, we show that the complexity class $\text{QIP}_{\text{EB}}(2)$ contains QAM [55] and QSZK [56]. It also follows, as a direct generalization of the hardness results from [5, 6], that the problem of estimating the fidelity of separability is hard for QSZK and NP. All of the aforementioned complexity classes are considered to be, in the worst case, out of reach of the capabilities of efficient quantum computers. See Appendix K for proofs and Figure 7 for a detailed diagram. However, following the approach of [57], we can try to solve some instances of problems in these classes using parameterized circuits and VQAs.

3 Conclusion and Discussion

In this paper, we detailed a distributed quantum computation to test the separability of a quantum state

that, at its core, uses quantum steering. This test demonstrated a link between quantum steering and the separability problem. The acceptance probability of this distributed quantum computation is directly related to an entanglement measure known as the fidelity of separability. Using the test's structure, we also showed computational complexity-theoretic results and established a link between quantum steering, quantum algorithms, and quantum computational complexity. By replacing the prover with a parameterized circuit, we modified this distributed quantum computation to develop our VQSA, a novel kind of variational quantum algorithm that uses quantum steering to address the problem of estimating the fidelity of separability. This algorithm allows for the direct estimation of the fidelity of separability without the need for state tomography and subsequent approximate tests on separability. Our algorithm is not unitary due to the mid-circuit measurement on system R and the consequent conditional operation applied on system A. This is an important distinction from most VQAs, which do not use a parameterized mid-circuit measurement. We also discuss multipartite generalizations of both our separability test and VQSA. Finally, we simulated our VQSA using the noisy Qiskit Aer simulator, which showed favorable convergence trends and was compared against two classical SDP benchmarks.

Our VQSA has applications beyond entanglement quantification on a single quantum computer. We can also think of our VQSA as a distributed variational quantum algorithm for measuring the entanglement of a bipartite state. See [58, 59, 60] for previous instances of distributed VQAs. Indeed, our algorithm can be executed over a quantum network in which each node has quantum and classical computers capable of performing VQAs. The initial part of the algorithm distributes R to Rob, A to Alice, and B to Bob, who are all in distant locations. Then, Rob performs the parameterized measurement and sends the outcome over a classical channel to Alice, who performs another parameterized measurement. Then, they can repeat this process to assess the quality of the entanglement between Alice and Bob. This interpretation is even more interesting regarding quantum networks for the multipartite case, in which the classical data gets broadcast from Rob to all the other nodes except the last one.

VQSAs can tackle other problems involving quantum steering, like maximizing the pure-state decompositions of quantum states. This technique may also be helpful for estimating other entanglement measures that involve optimizing the set of separable states. By applying the insights of [61, Appendix A] and our approach here, it is clear that VQSAs will also be helpful for estimating maximal fidelities associated with other resource theories, such as the resource theory of coherence [62]. More broadly, we suspect that the paradigm of parameterized mid-circuit measurements and distributed variational quantum algorithms will be helpful in addressing other computational problems of interest in quantum information science and physics, given recent advances in experimental implementations [63, 64, 65, 66].

Going forward from here, we consider it an important open question in quantum computational complexity theory to place a non-trivial upper bound on the class $\mathrm{QIP}_{\mathrm{EB}}(2)$. As indicated in Remark 7, an approach using the known quantum de Finetti theorem from [67, Theorem II.7'] does not appear to be helpful for this task.

4 Methods

This section briefly overviews the techniques used to prove Theorem 1, our main result, a brief description of SDP benchmarks, and essential details about our simulations.

To gain intuition about the separability test for mixed states, let us formulate a simple test for the separability of pure states. From (1), we can see that a pure bipartite state φ_{AB} is separable if it can be written in product form, as

$$\varphi_{AB} = \psi_A \otimes \phi_B, \tag{16}$$

where ψ_A and ϕ_B are pure states. The test we developed below is important because it will reappear as part of the test for separability in the general case, along with quantum steering. Additionally, our approach slightly differs from the standard approach for testing entanglement of pure states, which employs two copies of the state in a swap test [68, 69, 7]. Instead, our approach requires only a single copy of the state.

Our pure-state separability test consists of a distributed quantum computation involving a prover and a verifier (see Figure 8). The computation starts with the verifier preparing the pure state ψ_{AB}. The prover sends the verifier the pure state $\phi_{A'}$ in register A'. (We note that the prover can send a mixed state; however, the maximum acceptance probability of the test is achieved by a pure state. Hence, without loss of generality, the prover must send a pure state.) The verifier then performs the standard swap test [70, 71] on A and A' and accepts if the measurement outcome is zero. In the standard model of quantum computational complexity [41, 42], the prover attempts to get the verifier to accept the swap test with as high a probability as possible. Thus, in this scenario, the prover selects $\phi_{A'}$ to maximize the overlap between the reduced stated $\psi_A := \mathrm{Tr}_B[\psi_{AB}]$ and $\phi_{A'}$. The maximum acceptance

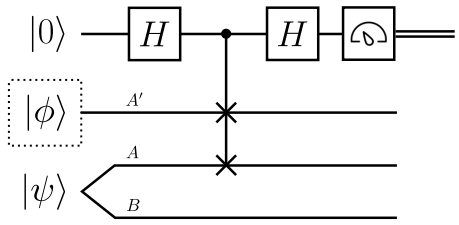


Figure 8: Pure-state separability test: The verifier has the pure state ψ_{AB} of interest. The prover (indicated by the dotted box) sends the verifier a pure state $\phi_{A'}$, who then performs the standard swap test on systems A' and A. As mentioned in (18), the acceptance probability is equal to $\frac{1}{2}(1 + \|\psi_A\|_\infty)$.

probability is then equal to

$$\begin{aligned}
&\max_{\phi} \operatorname{Tr}[(\Pi^{\text{sym}}_{A'A} \otimes I_B)(\phi_{A'} \otimes \psi_{AB})] \\
&= \frac{1}{2}\left(1 + \max_{\phi} \operatorname{Tr}[F_{A'A}(\phi_{A'} \otimes \psi_A)]\right) \qquad (17) \\
&= \frac{1}{2}\left(1 + \max_{\phi} \operatorname{Tr}[\phi_A \psi_A]\right) = \frac{1}{2}\left(1 + \|\psi_A\|_\infty\right), \qquad (18)
\end{aligned}$$

where $F_{A'A}$ is the unitary swap operator acting on systems A' and A, the projector $\Pi^{\text{sym}}_{A'A} \coloneqq \frac{1}{2}\left(I_{A'A} + F_{A'A}\right)$ projects onto the symmetric subspace of A' and A, and $\|\psi_A\|_\infty$ is the spectral norm of the reduced state ψ_A (equal to its largest eigenvalue). Since $\|\psi_A\|_\infty = 1$ if and only if ψ_A is a pure state and this occurs if and only if ψ_{AB} is a product state, it follows that the maximal acceptance probability is equal to one if and only if ψ_{AB} is a product state.

Now we outline the proof of Theorem 1, which relies on two important facts. The first is that the fidelity of separability can be written in terms of a convex roof as follows [61, Theorem 1]:

$$F_s(\rho_{AB}) = \max_{\substack{\{(p(x),\psi^x_{AB})\}_x, \\ \rho_{AB} = \sum_x p(x)\psi^x_{AB}}} \sum_x p(x) F_s(\psi^x_{AB}), \qquad (19)$$

where $\{p(x)\}_x$ is a probability distribution and each ψ^x_{AB} is a pure state. See also [72, Lemma 1]. The second fact is that, for a pure bipartite state, $F_s(\psi_{AB})$ can be rewritten as [61, Section 6.2]

$$F_s(\psi_{AB}) = \|\psi_A\|_\infty . \qquad (20)$$

Along with these facts, we also note that the optimization over all entanglement-breaking channels in (4) is the same as optimizing over all pure-state decompositions of ρ_{AB} and the rest of the proof follows. For completeness, we provide proofs of (19) and (20) in Appendices B and C, respectively. It follows from (1) and (20) that $\sum_x p(x) \|\psi^x_A\|_\infty = 1$ for a separable state, which is the maximum possible value of $F_s(\rho_{AB})$. Hence, the distributed quantum computation in Figure 1 tests and quantifies the separability of a state by estimating its fidelity of separability. Finally, note that the computation in Figure 1 can be reduced to that in Figure 8 if the purifying system R is trivial, implying that the verifier only prepares a pure state on systems A and B in this case.

Benchmarking via semidefinite programs—Here we briefly explain the derivation of the SDP benchmarks $\widetilde{F}^1_s(\rho_{AB}, k)$ and $\widetilde{F}^2_s(\rho_{AB}, k)$.

First, let us recall that the fidelity between two quantum states has an SDP formulation [73]. Since there is no semidefinite constraint that directly corresponds to optimizing over the set of separable states [74], we can approximate the fidelity of separability of a state by maximizing its fidelity with positive partial transpose (PPT) states [27, 28] and k-extendible states [29, 30]. Further noting that the PPT and k-extendibility constraints are positive semidefinite constraints, we obtain our first benchmark $\widetilde{F}^1_s(\rho_{AB}, k)$, defined in Appendix E, and which is proven there to satisfy the following bounds:

$$\begin{aligned}
&F_s(\rho_{AB}) \leq \widetilde{F}^1_s(\rho_{AB}, k) \\
&\leq 1 - \left[\sqrt{1 - F_s(\rho_{AB})} - 2\sqrt{\frac{|B|^2}{k}\left(1 - \frac{|B|^2}{k}\right)}\right]^2 , \qquad (21)
\end{aligned}$$

where $|B|$ is the dimension of system B. By inspection of the above inequalities, observe that

$$\lim_{k\to\infty} \widetilde{F}^1_s(\rho_{AB}, k) = F_s(\rho_{AB}). \qquad (22)$$

The second benchmark can be obtained using (4). Just like PPT and k-extendible states were used to approximate separable states for the first benchmark, we use PPT channels [75, 76] and k-extendible channels [77, 78, 79, 80] to approximate entanglement-breaking channels, leading to our second benchmark $\widetilde{F}^2_s(\rho_{AB}, k)$. We show that $\widetilde{F}^2_s(\rho_{AB}, k)$ is an SDP and approximates the fidelity of separability in the following fashion:

$$F_s(\rho_{AB}) \leq \widetilde{F}^2_s(\rho_{AB}, k) \leq F_s(\rho_{AB}) + \frac{4\,|A|^3\,|B|}{k}. \qquad (23)$$

where $|A|$ and $|B|$ is the dimension of systems A and B, respectively. See Appendix F for a proof. Again, observe that

$$\lim_{k\to\infty} \widetilde{F}^2_s(\rho_{AB}, k) = F_s(\rho_{AB}). \qquad (24)$$

Simulations and Reward Functions—For our simulations, we use the Qiskit Aer simulator and Qiskit's

Simultaneous Perturbation Stochastic Approximation (SPSA) optimizer to perform the classical optimization. The jitters in the fidelity values between iterations of the VQSA can be attributed to the shot noise in estimating the acceptance probability using the Qiskit Aer simulator, as well as the fact that the SPSA optimizer we have used to perform the classical optimization is itself a stochastic algorithm. We provide more examples in Appendix G.

An essential issue with variational quantum techniques, such as VQAs, is the emergence of barren plateaus or vanishing gradients as the number of qubits increases [43]. However, recent results have shown that this problem can be mitigated by switching from a global reward function to a local reward function [44]. In our case, a global reward function is one in which we measure all the qubits that constitute system A, as done in the approach discussed in Theorem 2. An example of a local reward function involves selecting a qubit in the system A at random to measure in the computational basis and recording the outcome, accepting if the result is equal to zero. Our proposed local reward function can be used to obtain upper and lower bounds on our initial global reward function, following the approach of [81, Appendix C] and discussed for completeness in Appendix L. Local functions have also been used to avoid barren plateaus in VQAs to determine the geometric measure of entanglement for pure states [82]. We provide simulations of the local reward function in Appendix G, indicating that the local reward function can also be used to estimate the fidelity of separability of a given state.

Acknowledgments

We are especially grateful to Gus Gutoski, for providing the main idea of the quantum interactive proof detailed in Figure 1, back in September 2013. We also thank Paul Alsing, Eric Chitambar, Zoe Holmes, and Wilfred Salmon for insightful discussions, and Ludovico Lami, Bartosz Regula, and Alexander Streltsov for the same, as well as pointing us to [72]. AP, SR, and MMW acknowledge support from the National Science Foundation under Grant No. 1907615.

References

[1] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?". Physical Review **47**, 777–780 (1935).

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

[3] Leonid Gurvits. "Classical deterministic complexity of Edmonds' problem and quantum entanglement". In Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing. Pages 10–19. San Diego, California, USA (2003).

[4] Sevag Gharibian. "Strong NP-hardness of the quantum separability problem". Quantum Information and Computation **10**, 343–360 (2010).

[5] Patrick Hayden, Kevin Milner, and Mark M. Wilde. "Two-message quantum interactive proofs and the quantum separability problem". In Proceedings of the 18th Annual IEEE Conference on Computational Complexity. Pages 156–167. Palo Alto, California, USA (2013).

[6] Patrick Hayden, Kevin Milner, and Mark M. Wilde. "Two-message quantum interactive proofs and the quantum separability problem". Quantum Information and Computation **14**, 384–416 (2014).

[7] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. "Quantum interactive proofs and the complexity of separability testing". Theory of Computing **11**, 59–103 (2015).

[8] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. "Entanglement in many-body systems". Reviews of Modern Physics **80**, 517–576 (2008).

[9] Marcus Cramer, Martin B. Plenio, and Harald Wunderlich. "Measuring entanglement in condensed matter systems". Physical Review Letters **106**, 020401 (2011).

[10] Nicolas Laflorencie. "Quantum entanglement in condensed matter systems". Physics Reports **646**, 1–59 (2016).

[11] Tadashi Takayanagi. "Entanglement entropy from a holographic viewpoint". Classical and Quantum Gravity **29**, 153001 (2012).

[12] Sougato Bose, Anupam Mazumdar, Gavin W. Morley, Hendrik Ulbricht, Marko Toroš, Mauro Paternostro, Andrew A. Geraci, Peter F. Barker, M. S. Kim, and Gerard Milburn. "Spin entanglement witness for quantum gravity". Physical Review Letters **119**, 240401 (2017).

[13] Chiara Marletto and Vlatko Vedral. "Gravitationally induced entanglement between two massive particles is sufficient evidence of quantum effects in gravity". Physical Review Letters **119**, 240402 (2017).

[14] Xiao-Liang Qi. "Does gravity come from quantum information?". Nature Physics **14**, 984–987 (2018).

[15] Brian Swingle. "Spacetime from entanglement". Annual Review of Condensed Matter Physics **9**, 345–358 (2018).

[16] Claude Fabre and Nicolas Treps. "Modes and states in quantum optics". Reviews of Modern Physics **92**, 035005 (2020).

[17] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". Physical Review Letters **67**, 661–663 (1991).

[18] Umesh Vazirani and Thomas Vidick. "Fully device-independent quantum key distribution". Physical Review Letters **113**, 140501 (2014).

[19] Charles H. Bennett and Stephen J. Wiesner. "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states". Physical Review Letters **69**, 2881 (1992).

[20] 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**, 1895 (1993).

[21] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. "Mixed state entanglement and quantum error correction". Physical Review A **54**, 3824–3851 (1996).

[22] Vlatko Vedral, Martin B. Plenio, M. A. Rippin, and Peter L. Knight. "Quantifying entanglement". Physical Review Letters **78**, 2275–2279 (1997).

[23] Vlatko Vedral and Martin B. Plenio. "Entanglement measures and purification procedures". Physical Review A **57**, 1619–1633 (1998).

[24] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki. "Quantum entanglement". Reviews of Modern Physics **81**, 865–942 (2009).

[25] J. P. Home, M. J. McDonnell, D. M. Lucas, G. Imreh, B. C. Keitch, D. J. Szwer, N. R. Thomas, S. C. Webster, D. N. Stacey, and A. M. Steane. "Deterministic entanglement and tomography of ion–spin qubits". New Journal of Physics **8**, 188–188 (2006).

[26] Matthias Steffen, M. Ansmann, Radoslaw C. Bialczak, N. Katz, Erik Lucero, R. McDermott, Matthew Neeley, E. M. Weig, A. N. Cleland, and John M. Martinis. "Measurement of the entanglement of two superconducting qubits via state tomography". Science **313**, 1423–1425 (2006).

[27] Asher Peres. "Separability criterion for density matrices". Physical Review Letters **77**, 1413–1415 (1996).

[28] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. "Separability of mixed states: necessary and sufficient conditions". Physics Letters A **223**, 1–8 (1996).

[29] Reinhard F. Werner. "An application of Bell's inequalities to a quantum state extension problem". Letters in Mathematical Physics **17**, 359–363 (1989).

[30] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Complete family of separability criteria". Physical Review A **69**, 022308 (2004).

[31] Margarite L. LaBorde, Soorya Rethinasamy, and Mark M. Wilde. "Testing symmetry on quantum computers". Quantum **7**, 1120 (2023).

[32] Erwin Schrödinger. "Die gegenwärtige situation in der quantenmechanik". Die Naturwissenschaften **23**, 844–849 (1935).

[33] Erwin Schrödinger. "Discussion of probability relations between separated systems". Mathematical Proceedings of the Cambridge Philosophical Society **31**, 555–563 (1935).

[34] Daniel Cavalcanti and Paul Skrzypczyk. "Quantum steering: a review with focus on semidefinite programming". Reports on Progress in Physics **80**, 024001 (2016).

[35] Roope Uola, Ana C. S. Costa, H. Chau Nguyen, and Otfried Gühne. "Quantum steering". Reviews of Modern Physics **92**, 015001 (2020).

[36] Shuheng Liu, Dongmei Han, Na Wang, Yu Xiang, Fengxiao Sun, Meihong Wang, Zhongzhong Qin, Qihuang Gong, Xiaolong Su, and Qiongyi He. "Experimental demonstration of remotely creating Wigner negativity via quantum steering". Physical Review Letters **128**, 200401 (2022).

[37] Marie Ioannou, Bradley Longstaff, Mikkel V. Larsen, Jonas S. Neergaard-Nielsen, Ulrik L. Andersen, Daniel Cavalcanti, Nicolas Brunner, and Jonatan Bohr Brask. "Steering-based randomness certification with squeezed states and homodyne measurements". Physical Review A **106**, 042414 (2022).

[38] Bernhard Wittmann, Sven Ramelow, Fabian Steinlechner, Nathan K. Langford, Nicolas Brunner, Howard M. Wiseman, Rupert Ursin, and Anton Zeilinger. "Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering". New Journal of Physics **14**, 053030 (2012).

[39] Meng Wang, Yu Xiang, Qiongyi He, and Qihuang Gong. "Detection of quantum steering in multipartite continuous-variable Greenberger-Horne-

Zeilinger–like states". Physical Review A **91**, 012112 (2015).

[40] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information". Cambridge University Press. (2000).

[41] John Watrous. "Quantum computational complexity". Encyclopedia of Complexity and System Science (2009).

[42] Thomas Vidick and John Watrous. "Quantum proofs". Foundations and Trends in Theoretical Computer Science **11**, 1–215 (2016).

[43] Jarrod R. McClean, Sergio Boixo, Vadim N. Smelyanskiy, Ryan Babbush, and Hartmut Neven. "Barren plateaus in quantum neural network training landscapes". Nature Communications **9**, 4812 (2018).

[44] Marco Cerezo, Akira Sone, Tyler Volkoff, Lukasz Cincio, and Patrick J. Coles. "Cost function dependent barren plateaus in shallow parametrized quantum circuits". Nature Communications **12**, 1791 (2021).

[45] Mirko Consiglio, Tony John George Apollaro, and Marcin Wieśniak. "Variational approach to the quantum separability problem". Physical Review A **106**, 062413 (2022).

[46] Xu-Fei Yin, Yuxuan Du, Yue-Yang Fei, Rui Zhang, Li-Zheng Liu, Yingqiu Mao, Tongliang Liu, Min-Hsiu Hsieh, Li Li, Nai-Le Liu, Dacheng Tao, Yu-Ao Chen, and Jian-Wei Pan. "Efficient bipartite entanglement detection scheme with a quantum adversarial solver". Physical Review Letters **128**, 110501 (2022).

[47] Kun Wang, Zhixin Song, Xuanqiang Zhao, Zihe Wang, and Xin Wang. "Detecting and quantifying entanglement on near-term quantum devices". npj Quantum Information **8**, 52 (2022).

[48] A. D. Muñoz Moller, L. Pereira, L. Zambrano, J. Cortés-Vega, and A. Delgado. "Variational determination of multiqubit geometrical entanglement in noisy intermediate-scale quantum computers". Physical Review Applied **18**, 024048 (2022).

[49] George Androulakis and Ryan McGaha. "Variational quantum algorithm for approximating convex roofs". Quantum Information and Computation **22**, 1081–1109 (2022).

[50] John Watrous. "The theory of quantum information". Cambridge University Press. (2018).

[51] Michal Horodecki, Peter W. Shor, and Mary Beth Ruskai. "Entanglement breaking channels". Reviews in Mathematical Physics **15**, 629–641 (2003).

[52] A. Uhlmann. "The "transition probability" in the state space of a $*$-algebra". Reports on Mathematical Physics **9**, 273–279 (1976).

[53] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles. "Variational quantum algorithms". Nature Reviews Physics **3**, 625–644 (2021).

[54] Sanjeev Arora and Boaz Barak. "Computational complexity: A modern approach". Cambridge University Press. (2009).

[55] Chris Marriott and John Watrous. "Quantum Arthur–Merlin games". In Proceedings of the 19th IEEE Annual Conference on Computational Complexity. Pages 275–285. IEEE (2004).

[56] John Watrous. "Zero-knowledge against quantum attacks". In Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing. Pages 296–305. (2006).

[57] Soorya Rethinasamy, Rochisha Agarwal, Kunal Sharma, and Mark M. Wilde. "Estimating distinguishability measures on quantum computers". Physical Review A **108**, 012409 (2023).

[58] Xuanqiang Zhao, Benchi Zhao, Zihe Wang, Zhixin Song, and Xin Wang. "Practical distributed quantum information processing with LOCCNet". npj Quantum Information **7**, 159 (2021).

[59] Brian Doolittle, R. Thomas Bromley, Nathan Killoran, and Eric Chitambar. "Variational quantum optimization of nonlocality in noisy quantum networks". IEEE Transactions on Quantum Engineering **4**, 1–27 (2023).

[60] Yun-Fei Niu, Shuo Zhang, Chen Ding, Wan-Su Bao, and He-Liang Huang. "Parameter-parallel distributed variational quantum algorithm". SciPost Phys. **14**, 132 (2023).

[61] Alexander Streltsov, Hermann Kampermann, and Dagmar Bruß. "Linking a distance measure of entanglement to its convex roof". New Journal of Physics **12**, 123004 (2010).

[62] Tillmann Baumgratz, Marcus Cramer, and Martin B. Plenio. "Quantifying coherence". Physical Review Letters **113**, 140401 (2014).

[63] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau. "Repeated quantum error correction on a continuously encoded qubit by real-time feedback". Nature Communications **7**, 11526 (2016).

[64] Laird Egan, Dripto M. Debroy, Crystal Noel, Andrew Risinger, Daiwei Zhu, Debopriyo Biswas, Michael Newman, Muyuan Li, Kenneth R. Brown, Marko Cetina, and Christopher Monroe. "Fault-tolerant control of an error-corrected qubit". Nature **598**, 281–286 (2021).

[65] Rajeev Acharya et al. "Suppressing quantum errors by scaling a surface code logical qubit". Nature **614**, 676–681 (2023).

[66] T. M. Graham, L. Phuttitarn, R. Chinnarasu, Y. Song, C. Poole, K. Jooya, J. Scott, A. Scott, P. Eichler, and M. Saffman. "Mid-circuit measurements on a neutral atom quantum processor" (2023). arXiv:2303.10051.

[67] Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner. "One-and-a-half quantum de Finetti theorems". Communications in Mathematical Physics **273**, 473–498 (2007).

[68] Gavin K. Brennen. "An observable measure of entanglement for pure states of multi-qubit systems". Quantum Information and Computation **3**, 619–626 (2003).

[69] Aram Harrow and Ashley Montanaro. "An efficient test for product states with applications to quantum Merlin–Arthur games". In Proceedings of the 51st Annual IEEE Symposium on the Foundations of Computer Science (FOCS). Pages 633–642. Las Vegas, Nevada, USA (2010).

[70] Adriano Barenco, André Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. "Stabilization of quantum computations by symmetrization". SIAM Journal on Computing **26**, 1541–1557 (1997).

[71] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. "Quantum fingerprinting". Physical Review Letters **87**, 167902 (2001).

[72] Bartosz Regula, Ludovico Lami, and Alexander Streltsov. "Nonasymptotic assisted distillation of quantum coherence". Physical Review A **98**, 052329 (2018).

[73] John Watrous. "Simpler semidefinite programs for completely bounded norms". Chicago Journal of Theoretical Computer Science (2013).

[74] Hamza Fawzi. "The set of separable states has no finite semidefinite representation except in dimension 3×2". Communications in Mathematical Physics **386**, 1319–1335 (2021).

[75] Eric M. Rains. "Bound on distillable entanglement". Physical Review A **60**, 179–184 (1999).

[76] Eric M. Rains. "A semidefinite program for distillable entanglement". IEEE Transactions on Information Theory **47**, 2921–2933 (2001).

[77] Lukasz Pankowski, Fernando G. S. L. Brandao, Michal Horodecki, and Graeme Smith. "Entanglement distillation by extendible maps". Quantum Information and Computation **13**, 751–770 (2013).

[78] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. "Extendibility limits the performance of quantum processors". Physical Review Letters **123**, 070502 (2019).

[79] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. "Resource theory of unextendibility and nonasymptotic quantum capacity". Physical Review A **104**, 022401 (2021).

[80] Mario Berta, Francesco Borderi, Omar Fawzi, and Volkher Scholz. "Semidefinite programming hierarchies for constrained bilinear optimization". Mathematical Programming **194**, 781–829 (2022).

[81] Sumeet Khatri, Ryan LaRose, Alexander Poremba, Lukasz Cincio, Andrew T. Sornborger, and Patrick J. Coles. "Quantum-assisted quantum compiling". Quantum **3**, 140 (2019).

[82] Leonardo Zambrano, Andrés Damián Muñoz-Moller, Mario Muñoz, Luciano Pereira, and Aldo Delgado. "Avoiding barren plateaus in the variational determination of geometric entanglement" (2023) arXiv:2304.13388.

[83] Alexey E. Rastegin. "Sine distance for quantum states" (2006) arXiv:quant-ph/0602112.

[84] Christopher A. Fuchs and Jeroen van de Graaf. "Cryptographic distinguishability measures for quantum-mechanical states". IEEE Transactions on Information Theory **45**, 1216 (1999).

[85] Joel J. Wallman and Steven T. Flammia. "Randomized benchmarking with confidence". New Journal of Physics **16**, 103032 (2014).

[86] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M. Chow, and Jay M. Gambetta. "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets". Nature **549**, 242–246 (2017).

[87] Guillaume Sagnol and Maximilian Stahlberg. "PICOS: A Python interface to conic optimization solvers". Journal of Open Source Software **7**, 3915 (2022).

[88] Lieven Vandenberghe. "The CVXOPT linear and quadratic cone program solvers". url: http://www.seas.ucla.edu/ vandenbe/publications/coneprog.pdf.

[89] Vincent Russo. "TOQITO–theory of quantum information toolkit: A python package for studying quantum information". Journal of Open Source Software **6**, 3082 (2021).

[90] Benjamin Schumacher. "Quantum coding". Physical Review A **51**, 2738–2747 (1995).

[91] Nilanjana Datta, Min-Hsiu Hsieh, and Mark M. Wilde. "Quantum rate distortion, reverse Shannon theorems, and source-channel separation". IEEE Transactions on Information Theory **59**, 615–630 (2013).

[92] Koenraad M. R. Audenaert, Christopher A. Fuchs, Christopher King, and Andreas Winter. "Multiplicativity of accessible fidelity and quantumness for sets of quantum states". Quantum Information and Computation **4**, 1–11 (2004).

[93] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. "Quantum cloning". Reviews of Modern Physics **77**, 1225–1256 (2005).

[94] John Watrous. "Limits on the power of quantum statistical zero-knowledge". In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science. Pages 459–468. (2002).

[95] Carl W. Helstrom. "Detection theory and quantum mechanics". Information and Control **10**, 254–291 (1967).

[96] Carl W. Helstrom. "Quantum detection and estimation theory". Journal of Statistical Physics **1**, 231–252 (1969).

A Proof of Theorem 1

In this appendix, we prove Theorem 1, showing that the acceptance probability of the first test of separability for mixed states is equal to $\frac{1}{2}\left(1 + F_s(\rho_{AB})\right)$.

Proof of Theorem 1. Recall that an entanglement-breaking channel can be rewritten as

$$\mathcal{E}_{R\to A'}(\cdot) = \sum_x \operatorname{Tr}[\mu_R^x(\cdot)]\phi_{A'}^x, \tag{25}$$

where $\{\mu_R^x\}_x$ is a rank-one POVM and $\{\phi_{A'}^x\}_x$ is a set of pure states. Then we find, for fixed $\mathcal{E}_{R\to A'}$, that

$$\begin{aligned}\operatorname{Tr}[\Pi_{A'A}^{\text{sym}}\mathcal{E}_{R\to A'}(\psi_{RAB})] &= \frac{1}{2}\operatorname{Tr}[(I_{A'A} + F_{A'A})\mathcal{E}_{R\to A'}(\psi_{RAB})] &(26)\\ &= \frac{1}{2}\left(1 + \operatorname{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]\right). &(27)\end{aligned}$$

So let us work with the expression $\operatorname{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]$. Consider that

$$\begin{aligned}\operatorname{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})] &= \operatorname{Tr}\left[F_{A'A}\sum_x \operatorname{Tr}_R[\mu_R^x\psi_{RAB}]\otimes\phi_{A'}^x\right] &(28)\\ &= \operatorname{Tr}\left[F_{A'A}\sum_x p(x)\psi_{AB}^x\otimes\phi_{A'}^x\right] &(29)\\ &= \operatorname{Tr}\left[F_{A'A}\sum_x p(x)\psi_{A}^x\otimes\phi_{A'}^x\right] &(30)\\ &= \sum_x p(x)\langle\phi^x|_A\psi_A^x|\phi^x\rangle_A, &(31)\end{aligned}$$

where

$$p(x) := \operatorname{Tr}[\mu_R^x\psi_{RAB}], \tag{32}$$

$$\psi_{AB}^{x} \coloneqq \frac{1}{p(x)} \operatorname{Tr}_R[\mu_R^x \psi_{RAB}]. \tag{33}$$

Thus, the acceptance probability for a fixed entanglement-breaking channel is given by

$$\operatorname{Tr}[\Pi_{A'A}^{\text{sym}} \mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1}{2}\left(1 + \sum_x p(x) \langle \phi^x|_A \psi_A^x |\phi^x\rangle_A\right). \tag{34}$$

After optimizing over every element of $\text{EB}_{R\to A'}$, which denotes the set of all entanglement-breaking channels with input system R and output system A', and realizing that optimizing over measurements in $\mathcal{E}_{R\to A'}$ induces a pure-state decomposition of ρ_{AB} and optimizing over preparation channels in $\mathcal{E}_{R\to A'}$ gives the spectral norm of ψ_A^x, we find the claimed formula for the acceptance probability, when combined with the development in Appendices B and C:

$$\max_{\mathcal{E}\in \text{EB}_{R\to A'}} \operatorname{Tr}[(\Pi_{A'A}^{\text{sym}} \otimes I_{RB}) \mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1 + F_s(\rho_{AB})}{2}. \tag{35}$$

This concludes the proof. ■

B Alternative Proof of Equation (19)

This appendix provides an alternative proof for Theorem 1 in [61]. This proof relies on Uhlmann's theorem [52], the triangle inequality, and the Cauchy–Schwarz inequality. See also [72, Lemma 1].

Theorem 4 ([61]) *The following formula holds*

$$F_s(\rho_{AB}) = \max_{\{(p(x),\psi_{AB}^x)\}_x} \left\{ \sum_x p(x) F_s(\psi_{AB}^x) : \rho_{AB} = \sum_x p(x) \psi_{AB}^x \right\}, \tag{36}$$

where $\{(p(x), \psi_{AB}^x)\}_x$ *satisfies* $\sum_x p(x)\psi_{AB}^x = \rho_{AB}$*, all* ψ_{AB}^x *are pure, and*

$$F_s(\psi_{AB}) = \max_{|\phi\rangle_A, |\varphi\rangle_B} |\langle \psi|_{AB} |\phi\rangle_A \otimes |\varphi\rangle_B|^2. \tag{37}$$

Proof. Since the definition in (5) requires an optimization over all separable states, we take $|\mathcal{X}| = (|A|\,|B|)^2$. The separable state in (1) is purified by

$$|\psi^\sigma\rangle_{RAB} = \sum_{x\in\mathcal{X}} \sqrt{p(x)} |x\rangle_R |\psi^x\rangle_A |\phi^x\rangle_B. \tag{38}$$

Now consider a generic purification $|\psi^\rho\rangle_{R'AB}$ of ρ_{AB}. Recall that the dimension of the purifying system R' satisfies $\operatorname{rank}(\rho_{AB}) \leq |R'|$ and so we can simply set $|R'| = |A|\,|B|$. Taking R'' to be a system of dimension $|A|\,|B|$, we then have that

$$|\psi^\rho\rangle_{R'AB} |0\rangle_{R''} \tag{39}$$

purifies ρ_{AB}. Applying Uhlmann's theorem [52], the maximum separable root fidelity can be written as

$$\max_{\sigma_{AB}\in \text{SEP}(A:B)} \sqrt{F}(\rho_{AB}, \sigma_{AB}) =$$

$$\max_{\substack{U,\\ \{(p(x),\psi^x{}_A,\phi^x_B)\}_x}} \left| \left(\sum_{x'} \sqrt{p(x')} \langle x'|_R \langle \psi^{x'}|_A \langle \phi^{x'}|_B \right) \left(U_{R'R''\to R} \otimes I_{AB} \right) |\psi^\rho\rangle_{R'AB} |0\rangle_{R''} \right|, \quad (40)$$

where the maximization is over every unitary $U_{R'R''\to R}$. Expanding $U_{R'R''\to R}|\psi^\rho\rangle_{R'AB}|0\rangle_{R''}$ in terms of the standard basis $|x\rangle$ as

$$U_{R'R''\to R}|\psi^\rho\rangle_{R'AB}|0\rangle_{R''} = \sum_{x\in\mathcal{X}} \sqrt{q(x)}|x\rangle_R|\varphi^x\rangle_{AB}, \quad (41)$$

we note that U followed by a measurement in the standard basis induces a convex decomposition of ρ_{AB} in terms of the ensemble $\{(q(x), \varphi^x_{AB})\}_x$. We can write the root fidelity as

$$\begin{aligned}
\max_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \sqrt{F}(\rho_{AB}, \sigma_{AB}) &= \max_{\substack{\{(p(x),\psi^x{}_A,\phi^x_B)\}_x,\\ \{(q(x),\varphi^x_{AB})\}_x}} \left| \sum_{x,x'} \sqrt{q(x)p(x')} \langle x|x'\rangle_R \langle \varphi^x|_{AB} |\psi^{x'}\rangle_A |\phi^{x'}\rangle_B \right| \\
&= \max_{\substack{\{(p(x),\psi^x{}_A,\phi^x_B)\}_x,\\ \{(q(x),\varphi^x_{AB})\}_x}} \left| \sum_{x} \sqrt{q(x)p(x)} \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right| \quad (42) \\
&= \max_{\substack{\{(p(x),\psi^x{}_A,\phi^x_B)\}_x,\\ \{(q(x),\varphi^x_{AB})\}_x}} \left| \sum_{x} \sqrt{q(x)p(x)} \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right|. \quad (43)
\end{aligned}$$

Next, for fixed $\{(p(x), \psi^x{}_A, \phi^x_B)\}_x$ and $\{(q(x), \varphi^x_{AB})\}_x$, we bound the objective function in the optimization above as follows:

$$\begin{aligned}
\left| \sum_{x} \sqrt{q(x)p(x)} \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right| &\leq \sum_x \sqrt{p(x)q(x)} \left| \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right| \quad (44) \\
&\leq \sqrt{\sum_x p(x)} \sqrt{\sum_x q(x) \left| \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right|^2} \quad (45) \\
&= \sqrt{\sum_x q(x) \left| \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right|^2}. \quad (46)
\end{aligned}$$

The first inequality follows from the triangle inequality, and the second from an application of Cauchy–Schwarz. We see that equality is achieved in the second inequality by choosing

$$p(x) = \frac{q(x) \left| \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right|^2}{\sum_x q(x) \left| \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right|^2}. \quad (47)$$

We can achieve equality in the first inequality by tuning a global phase for the state $|\psi^x\rangle_A$, which amounts to a relative phase in (38). Putting everything together, we conclude that

$$\max_{\sigma_{AB}\in \mathrm{SEP}} F(\rho_{AB}, \sigma_{AB}) = \max_{\{(q(x),\varphi^x_{AB})\}_x} \sum_x q(x) \max_{(|\psi^x\rangle_A |\phi^x\rangle_B)_x,} \left| \langle \varphi^x|_{AB} |\psi^x\rangle_A |\phi^x\rangle_B \right|^2, \quad (48)$$

which is equivalent to the desired equality in (19). ∎

C Proof of Equation (20)

In this appendix, we show that the fidelity of separability of a bipartite state can be written in terms of the spectral norm, which was also observed in [61, Section 6.2].

Proposition 5 *For a bipartite state, the following equality holds*

$$F_s(\rho_{AB}) = \max_{\left\{(p(x),\psi^x_{AB})\right\}_x} \left\{ \sum_x p(x) \left\|\psi^x_A\right\|_\infty : \rho_{AB} = \sum_x p(x)\psi^x_{AB} \right\}. \tag{49}$$

Proof. Consider that the following holds for a pure bipartite state ψ_{AB}:

$$\begin{aligned} F_s(\psi_{AB}) &= \max_{|\phi\rangle_A, |\varphi\rangle_B} \left|\langle\psi|_{AB} |\phi\rangle_A \otimes |\varphi\rangle_B\right|^2 && (50)\\ &= \max_{|\phi\rangle_A, |\varphi\rangle_B} \left|\langle\phi|_A \otimes \langle\varphi|_B |\psi\rangle_{AB}\right|^2 && (51)\\ &= \max_{|\phi\rangle_A} \left\|\langle\phi|_A \otimes I_B |\psi\rangle_{AB}\right\|_2^2 && (52)\\ &= \max_{|\phi\rangle_A} \operatorname{Tr}[(|\phi\rangle\langle\phi|_A \otimes I_B)\psi_{AB}] && (53)\\ &= \max_{|\phi\rangle_A} \operatorname{Tr}[|\phi\rangle\langle\phi|_A \psi_A] && (54)\\ &= \left\|\psi_A\right\|_\infty . && (55) \end{aligned}$$

The first two equalities follow from the definition and a rewriting. The third equality follows from the variational characterization of the Euclidean norm of a vector. The fourth equality follows because

$$\begin{aligned} \left\|\langle\phi|_A \otimes I_B |\psi\rangle_{AB}\right\|_2^2 &= \left(\langle\psi|_{AB} |\phi\rangle_A \otimes I_B\right)\left(\langle\phi|_A \otimes I_B |\psi\rangle_{AB}\right) && (56)\\ &= \langle\psi|_{AB} |\phi\rangle\langle\phi|_A \otimes I_B |\psi\rangle_{AB} && (57)\\ &= \operatorname{Tr}[(|\phi\rangle\langle\phi|_A \otimes I_B)\psi_{AB}]. && (58) \end{aligned}$$

The next step follows by taking a partial trace and the final equality from the variational characterization of the spectral norm. So this implies the desired equality after applying (19). ∎

D Proof of Theorem 2

In this appendix, we show that the acceptance probability of our VQSA is indeed equal to $F_s(\rho_{AB})$ if the parameterized unitary circuits can express all possible unitary operators of their respective systems. For this, let us track the state of the VQSA at the points indicated in Figure 9.

- At Step (1), the unitary U^ρ prepares the pure state ψ_{RAB}. This is a specific initial purification of ρ_{AB}.
- At Step (2), we apply the parameterized unitary circuit $W_R(\Theta)$ to ψ_{RAB}. Expanding $W_R(\Theta)|\psi^\rho\rangle_{RAB}$ in terms of the standard basis $\{|x\rangle\}_x$ leads to

$$W_R(\Theta)|\psi\rangle_{RAB} = \sum_{x\in\mathcal{X}} \sqrt{q(x)}|x\rangle_R |\varphi^x\rangle_{AB}. \tag{59}$$

- At Step (3), the measurement outcome x occurs with probability $q(x)$, and the state vector of registers A and B becomes $|\varphi^x\rangle_{AB}$.
- At Step (4), depending on the measurement outcome x, we apply the parameterized unitary circuit $U^x_A(\Theta^x)$ to register A. The state vector is now $U^x_A(\Theta^x)|\varphi^x\rangle_{AB}$.

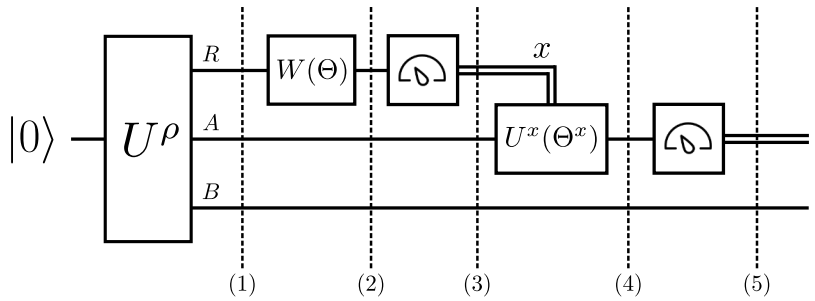


Figure 9: VQSA to estimate the fidelity of separability $F_s(\rho_{AB})$. The unitary circuit U^ρ produces the state ψ_{RAB}, which is a purification of ρ_{AB}. The parameterized circuit $W_R(\Theta)$ acts on R to evolve ψ_{RAB} to another pure-state decomposition of ρ_{AB}. The following measurement steers the system AB to be in a pure state ψ^x_{AB} if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuit $U^x_A(\Theta^x)$ and the subsequent measurement estimates $\|\psi^x_A\|_\infty$.

- At Step (5), we trace over B and measure A in the standard basis. We accept when we get the all-zeros outcome. The acceptance probability is then equal to

$$\sum_{x\in\mathcal{X}} q(x) \langle 0| U^x_A(\Theta^x)\varphi^x_A (U^x_A)^\dagger |0\rangle = \sum_{x\in\mathcal{X}} q(x) \langle \phi^x|_A \varphi^x_A |\phi^x\rangle_A, \tag{60}$$

  where we have defined $|\phi^x\rangle_A \coloneqq (U^x_A)^\dagger |0\rangle$.

- Maximizing the acceptance probability corresponds to maximization over the parameters of $W_R(\Theta)$ and $U^x_A(\Theta^x)$.

- Maximization over the parameters of W_R is a maximization over all possible pure-state decompositions of ρ_{AB}.

- Maximization over the parameters of $U^x_A(\Theta^x)$ is a maximization of $\langle\phi^x|\varphi^x_A|\phi^x\rangle$, which yields the value of $\|\varphi^x_A\|_\infty$.

- The maximum acceptance probability is equal to

$$\max_{\left\{(p(x),\psi^x_{AB})\right\}_x} \left\{ \sum_x p(x) \|\varphi^x_A\|_\infty : \rho_{AB} = \sum_x p(x)\psi^x_{AB} \right\}, \tag{61}$$

  which is in turn equal to $F_s(\rho_{AB})$, by Proposition 5.

This proves that if the parameterized unitary circuits can express all possible unitary operators of their respective systems, the maximum acceptance probability equals $F_s(\rho_{AB})$. However, we note that any ansatz employed for the parameterized unitary circuits has limited expressibility. As such, the maximum acceptance probability obtained via the VQSA will also be closer to the actual value of $F_s(\rho_{AB})$ if we use a more expressive ansatz.

E First Benchmarking SDP $\widetilde{F}^1_s$ and Proof of Equation (21)

This appendix details the derivation of our first benchmarking SDP $\widetilde{F}^1_s$, based on the SDP for fidelity [73]. Let ρ_{AB} and σ_{AB} be bipartite states. The SDP for the root fidelity $\sqrt{F}(\rho_{AB},\sigma_{AB})$, which makes use of Uhlmann's theorem [52], is as follows:

$$\sqrt{F}(\rho_{AB},\sigma_{AB}) = \max_{X_{AB}\in\mathcal{L}(\mathcal{H}_{AB})} \left\{ \operatorname{Re}[\operatorname{Tr}[X_{AB}]] : \begin{bmatrix} \rho_{AB} & X_{AB} \\ X^\dagger_{AB} & \sigma_{AB} \end{bmatrix} \geq 0 \right\}, \tag{62}$$

where $\mathcal{L}(\mathcal{H}_{AB})$ is the set of all linear operators acting on the Hilbert space $\mathcal{H}_{AB}$.

We would ideally like to include a maximization over the set of all separable states, but it is well known to be computationally challenging to optimize over this set [3, 4]. Note that it is not generally possible to characterize the set of separable states using semi-definite constraints [74]. Instead, we can only approximate the set by constraining σ_{AB} to have a positive partial transpose (PPT) [27, 28] and be k-extendible [29, 30], since all separable states satisfy these constraints. Let $\widetilde{F}_s^1(\rho_{AB})$ denote the resulting quantity, the square root of which is defined as follows:

$$\sqrt{\widetilde{F}_s^1}(\rho_{AB},k) \coloneqq \max_{\substack{X_{AB}\in\mathcal{L}(\mathcal{H}_{AB}),\\ \sigma_{AB^k}\geq 0}} \left\{ \begin{array}{c} \operatorname{Re}[\operatorname{Tr}[X_{AB}]] : \\ \begin{bmatrix} \rho_{AB} & X_{AB} \\ X_{AB}^\dagger & \sigma_{AB_1} \end{bmatrix} \geq 0, \\ \operatorname{Tr}[\sigma_{AB^k}] = 1, \\ \sigma_{AB^k} = \mathcal{P}_{B^k}(\sigma_{AB^k}), \\ T_{B_{1\cdots j}}(\sigma_{AB_{1\cdots j}}) \geq 0 \quad \forall j \leq k \end{array} \right\}, \tag{63}$$

where $B^k \equiv B_1 \cdots B_k$, the notation T_R denotes the partial transpose map acting on system R, and $\mathcal{P}_{B^k}$ denotes the channel that performs a uniformly random permutation of systems B_1 through B_k.

We prove the inequalities in (21). Due to the containment discussed above, we note that

$$F_s(\rho_{AB}) \leq \widetilde{F}_s^1(\rho_{AB},k). \tag{64}$$

An opposite bound on $\widetilde{F}_s^1(\rho_{AB},k)$ in terms of $F_s(\rho_{AB})$ is as follows:

$$\sqrt{1-F_s(\rho_{AB})} \leq \sqrt{1-\widetilde{F}_s^1(\rho_{AB},k)} + 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)}, \tag{65}$$

which can be rewritten as

$$\widetilde{F}_s^1(\rho_{AB},k) \leq 1 - \left[\sqrt{1-F_s(\rho_{AB})} - 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)}\right]^2. \tag{66}$$

It is a consequence of [67, Theorem II.7], the triangle inequality for sine distance [83], and the Fuchs-van-de-Graaf inequalities [84]. Indeed, consider that

$$\begin{aligned} \widetilde{F}_s^1(\rho_{AB},k) &= \max_{\sigma_{AB}\in\text{EXT-PPT}_k} F(\rho_{AB},\sigma_{AB}) && (67)\\ &\leq \max_{\sigma_{AB}\in\text{EXT}_k} F(\rho_{AB},\sigma_{AB}), && (68)\end{aligned}$$

where EXT-PPT$_k$ denotes the set being optimized over in (63) and EXT$_k$ is the set of k-extendible states. Now recall that for all $\omega_{AB}^k \in \text{EXT}_k$ [67, Theorem II.7']

$$\min_{\sigma_{AB}\in\text{SEP}(A:B)} \frac{1}{2}\left\|\omega_{AB}^k - \sigma_{AB}\right\|_1 \leq \frac{2\,|B|^2}{k}, \tag{69}$$

the sine distance obeys the triangle inequality [83]:

$$\sqrt{1-F(\omega,\tau)} \leq \sqrt{1-F(\omega,\xi)} + \sqrt{1-F(\xi,\tau)}, \tag{70}$$

and the Fuchs-van-de-Graaf inequality [84]:

$$1-\sqrt{F}(\omega,\tau) \leq \frac{1}{2}\left\|\omega-\tau\right\|_1, \tag{71}$$

where ω, τ, and ξ are states. If $\frac{1}{2}\left\|\omega-\tau\right\|_1 \leq \varepsilon$, the latter implies that

$$1-\sqrt{F}(\omega,\tau) \leq \varepsilon \;\Leftrightarrow\; \sqrt{1-F(\omega,\tau)} \leq \sqrt{\varepsilon\,(2-\varepsilon)}. \tag{72}$$

Letting σ_{AB}^k be an optimal choice in (68) and σ'_{AB} an optimal choice for $\min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \frac{1}{2}\left\|\omega_{AB}^k-\sigma_{AB}\right\|_1$, this implies that

$$\begin{aligned}
\min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \sqrt{1-F(\rho_{AB},\sigma_{AB})} &\leq \sqrt{1-F(\rho_{AB},\sigma'_{AB})} && (73)\\
&\leq \sqrt{1-F(\rho_{AB},\sigma_{AB}^k)}+\sqrt{1-F(\sigma'_{AB},\sigma_{AB}^k)} && (74)\\
&\leq \sqrt{1-F(\rho_{AB},\sigma_{AB}^k)}+2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)}. && (75)
\end{aligned}$$

Rearranging and applying (67)–(68), we arrive at the claimed inequality in (65).

F Second Benchmarking SDP $\widetilde{F}_s^2$ and Proof of Equation (23)

In this appendix, we detail the derivation of our second benchmark SDP $\widetilde{F}_s^2$, which is an SDP that approximates (4) in the main text. Consider a version of the distributed quantum computation that led to (4) where, instead of restricting the prover to only entanglement-breaking channels, we insist that the prover sends back k systems labeled as $A_1\cdots A_k$. Then, the verifier randomly selects one of the k systems and performs a swap test on the A system of the state ψ_{RAB}. This random selection is conducted so that the prover output is effectively reduced to that of an approximate entanglement-breaking channel. Note that the resulting interactive proof is in QIP(2). More specifically, the acceptance probability of this interactive proof system is given by

$$\max_{\mathcal{P}_{R\to A'_1\cdots A'_k}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\overline{\mathcal{P}}_{R\to A'}(\psi_{RAB})], \tag{76}$$

where

$$\overline{\mathcal{P}}_{R\to A'} := \frac{1}{k}\sum_{i=1}^{k} \mathrm{Tr}_{A_1^{k\prime}\setminus A_i}\circ\mathcal{P}_{R\to A'_1\cdots A'_k}, \tag{77}$$

and $\mathcal{P}$ is a preparation channel. Observing that $\overline{\mathcal{P}}_{R\to A'}$ is a k-extendible channel [77, 78, 79, 80], it follows that

$$\begin{aligned}
\max_{\mathcal{P}_{R\to A'_1\cdots A'_k}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\overline{\mathcal{P}}_{R\to A'}(\psi_{RAB})] &= \max_{\mathcal{E}^k_{R\to A'}\in \mathrm{EXT}_k} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\mathcal{E}^k_{R\to A'}(\psi_{RAB})] && (78)\\
&=: \frac{1}{2}(1+\widetilde{F}_s^2(\rho_{AB},k)), && (79)
\end{aligned}$$

where EXT_k denotes the set of k-extendible channels. These are defined by $\mathcal{E}^k_{R\to A'}(\rho_{SR})\in \mathrm{EXT}_k(S:A')$ for every input state ρ_{SR}, where $\mathrm{EXT}_k(S:A')$ denotes the set of k-extendible states. Hence, we estimate (4) using $\widetilde{F}_s^2(\rho_{AB},k)$ and it is given by the following SDP:

$$\frac{1}{2}(1+\widetilde{F}_s^2(\rho_{AB},k)) = \max_{\Gamma^{\mathcal{E}^k}_{RA'^k}\geq 0} \left\{ \begin{array}{c} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\,\mathrm{Tr}_R[T_R(\psi_{RAB})\Gamma^{\mathcal{E}^k}_{RA'_1}]] : \\ \mathrm{Tr}_{A'^k}[\Gamma^{\mathcal{E}^k}_{RA'^k}] = I_R, \\ \Gamma^{\mathcal{E}^k}_{RA'^k} = \mathcal{P}_{A'^k}(\Gamma^{\mathcal{E}^k}_{RA'^k}), \\ T_{A'_{1\cdots j}}(\Gamma^{\mathcal{E}^k}_{RA'^k}) \geq 0 \quad \forall j\leq k \end{array} \right\}, \tag{80}$$

where $\Gamma^{\mathcal{E}^k}_{RA'}$ is the Choi operator of $\mathcal{E}^k$, the map T_R is the partial transpose map acting on system R, and $\mathcal{P}_{A'^k}$ is the channel that randomly permutes the systems A'^k.

The following theorem indicates how $\widetilde{F}^2_s$ approximates $F_s(\rho_{AB})$.

Proposition 6 *The following bound holds for a bipartite state ρ_{AB}:*

$$F_s(\rho_{AB}) \leq \widetilde{F}^2_s(\rho_{AB}, k) \leq F_s(\rho_{AB}) + \frac{4\left|A\right|^3 \left|B\right|}{k}. \tag{81}$$

Proof. Since every entanglement-breaking channel is k-extendible, we trivially find that

$$\begin{aligned}
\frac{1 + F_s(\rho_{AB})}{2} &= \max_{\mathcal{E} \in \mathrm{EB}} \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}) \mathcal{E}_{R\to A'}(\psi_{RAB})] && (82)\\
&\leq \max_{\mathcal{E}^k_{R\to A'} \in \mathrm{EXT}_k} \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}) \mathcal{E}^k_{R\to A'}(\psi_{RAB})] && (83)\\
&= \frac{1 + \widetilde{F}^2_s(\rho_{AB}, k)}{2}. && (84)
\end{aligned}$$

Consider the following bound for a k-extendible state ω^k_{AB} [67, Theorem II.7']:

$$\min_{\sigma_{AB} \in \mathrm{SEP}(A:B)} \frac{1}{2} \left\| \omega^k_{AB} - \sigma_{AB} \right\|_1 \leq \frac{2\left|B\right|^2}{k}. \tag{85}$$

We can use it and the result of [85, Lemma 7] to conclude that

$$\min_{\mathcal{E} \in \mathrm{EB}} \frac{1}{2} \left\| \mathcal{E}^k - \mathcal{E} \right\|_\diamond \leq \frac{2\left|R\right| \left|A'\right|^2}{k}. \tag{86}$$

Then consider, for every fixed choice of $\mathcal{E}^k_{R\to A'}$, there exists an entanglement-breaking channel $\mathcal{E}$ satisfying

$$\frac{1}{2} \left\| \mathcal{E}^k - \mathcal{E} \right\|_\diamond \leq \frac{2\left|R\right| \left|A'\right|^2}{k}. \tag{87}$$

Then we find that

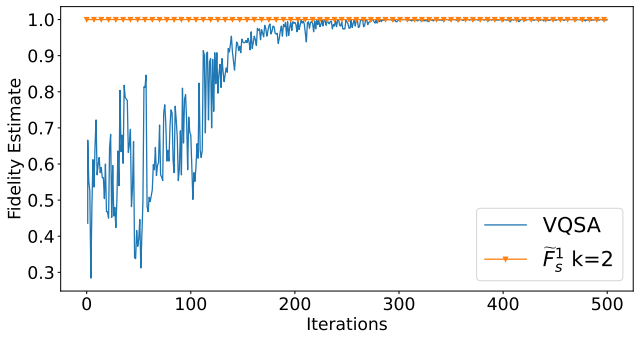
$$\begin{aligned}
&\mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}) \mathcal{E}^k_{R\to A'}(\psi_{RAB})] \\
&\leq \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}) \mathcal{E}_{R\to A'}(\psi_{RAB})] + \frac{2\left|R\right| \left|A'\right|^2}{k} && (88)\\
&\leq \max_{\mathcal{E} \in \mathrm{EB}} \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}) \mathcal{E}_{R\to A'}(\psi_{RAB})] + \frac{2\left|R\right| \left|A'\right|^2}{k} && (89)\\
&= \frac{1 + F_s(\rho_{AB})}{2} + \frac{2\left|R\right| \left|A'\right|^2}{k}. && (90)
\end{aligned}$$

Since the inequality holds for every $\mathcal{E}^k_{R\to A'} \in \mathrm{EXT}_k$, it follows that

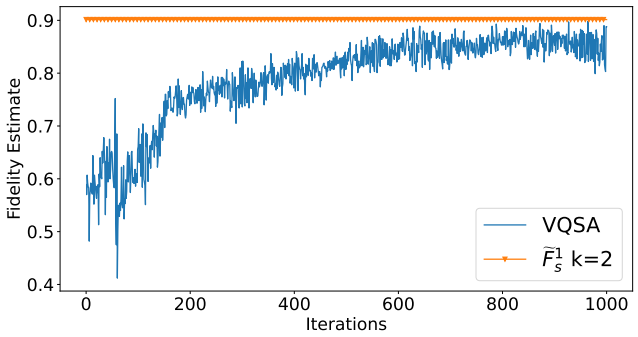
$$\max_{\mathcal{E}^k_{R\to A'} \in \mathrm{EXT}_k} \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}) \mathcal{E}^k_{R\to A'}(\psi_{RAB})] \leq \frac{1 + F_s(\rho_{AB})}{2} + \frac{2\left|R\right| \left|A'\right|^2}{k}. \tag{91}$$

This concludes the proof after recalling that $|R| \leq |A||B|$, observing that $|A| = |A'|$, and performing some simple algebra. ■

Remark 7 *Although the correction term in the upper bound in Proposition 6 decreases with increasing k, it is clear that, for it to become arbitrarily small, k needs to be larger than $|A|^3|B|$, which is exponential in the number of qubits for the state ρ_{AB}. Thus, this approach does not lead to an efficient method for placing the fidelity of separability estimation problem in QIP(2) or even QIP.*



(a) Fidelity of separability calculated for a random product state using the local reward function of the VQSA and benchmarked by $\widetilde{F}_s^1$.



(b) Fidelity of separability calculated for a random entangled state using the local reward function of the VQSA and benchmarked by $\widetilde{F}_s^1$.

Figure 10: Fidelity of separability estimated using the local reward function of the VQSA and benchmarked by $\widetilde{F}_s^1$.

G Further Simulations and Details

For all the simulations in our work, the input states and the parameterized unitaries are generated using the hardware efficient ansatz (HEA) [86]. The HEA consists of several layers, where each layer consists of two parameters per qubit per layer, specifying rotations about the x- and y-axes. After each layer of rotations is a series of neighboring qubit CNOT gates. When using the HEA to generate the input states, we keep the rotation angles fixed, thus leading to a fixed input state. For the parameterized unitaries, the rotation angles are parameters and are optimized over.

In Figure 10(a), we report simulation results after generating a random bipartite product state, with each partition containing two qubits. To guarantee a product state, we remove all the CNOT gates from the HEA that generates the input state ρ. We calculated the fidelity of separability using both the local reward function of the VQSA and the benchmark $\widetilde{F}_s^1$, the latter discussed in Appendix E.

In Figure 10(b), we do the same for a random bipartite state with the partitions A and B containing two qubits and one qubit, respectively, and three qubits in the reference system.

We generated all parameterized unitary circuits in the following fashion. We used the Qiskit Aer simulator and Qiskit's Simultaneous Perturbation Stochastic Approximation (SPSA) optimizer to perform the classical optimization. All other details can be found in Table 1. The local reward function of the VQSA requires more classical processing (like picking a qubit at random to measure) and seems to require more iterations to reach the right value. However, these downsides are outweighed by the fact that it is less susceptible to the emergence of barren plateaus. More details about the local cost function can be found in Appendix L.

H Software

All of our Python source files are available with the arXiv posting of this paper. We performed all simulations using the noisy Qiskit Aer simulator. The Picos Python package [87] was used to invoke the CVXOPT solver [88] for solving the SDPs, and the toqito Python package [89] was used for carrying out specific operations on the matrices representing quantum systems.

Figure	No. of Qubits	State ρ_{AB}	Layer Count
3	$R=2,\ A=1,\ B=1$	$(3/4)\|\Phi^+\rangle\langle\Phi^+\| + (1/4)\|\Phi^-\rangle\langle\Phi^-\|$	W_R no. of layers $= 2$ U_A^x no. of layers $= 2$
4	$R=4,\ A=2,\ B=2$	$(\mathcal{D}_{p,A_1} \otimes \mathcal{D}_{p,A_2} \otimes \mathbb{I}_B)(\|\psi\rangle\langle\psi\|)$ $\|\psi\rangle = \frac{1}{\sqrt{2}}(\|0\rangle_{A_1}\|0\rangle_{A_2}\|00\rangle_B + \|1\rangle_{A_1}\|1\rangle_{A_2}\|11\rangle_B)$	W_R no. of layers $= 4$ U_A^x no. of layers $= 4$
10(a)	$R=3,\ A=2,\ B=2$	Random product state using HEA [86]	W_R no. of layers $= 4$ U_A^x no. of layers $= 4$
10(b)	$R=3,\ A=2,\ B=2$	Random entangled state using HEA [86]	W_R no. of layers $= 4$ U_A^x no. of layers $= 4$

Table 1: Details of all VQSA simulations.

I Multipartite Scenarios

In this appendix, we discuss a multipartite generalization of mixed states' separability tests.

Definition 8 *A state $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M}) = \mathcal{D}(\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_M})$ is separable if it can be written as*

$$\rho_{A_1\cdots A_M} = \sum_{x\in\chi} p(x)\psi_{A_1}^{x,1} \otimes \cdots \otimes \psi_{A_M}^{x,M}, \tag{92}$$

where $\psi_{A_i}^{x,i}$ is a pure state for every $x \in \mathcal{X}$ and $i \in \{1,\ldots,M\}$.

Let M-SEP denote the set of all $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M})$ such that $\rho_{A_1\cdots A_M}$ is separable. The following theorem is important for the rest of this analysis.

Theorem 9 ([61]) *The following formula holds*

$$\max_{\sigma_{A_1\cdots A_M}\in M-\text{SEP}} F(\rho_{A_1\cdots A_M}, \sigma_{A_1\cdots A_M}) = \max_{\{(q(x),\varphi^x_{A_1\cdots A_M})\}_x} \sum_x q(x) F_s(\varphi^x_{A_1\cdots A_M}), \tag{93}$$

where the optimization is over every pure-state decomposition $\{(q(x),\varphi^x_{A_1\cdots A_M})\}_x$ of $\rho_{A_1\cdots A_M}$ (similar to those in Theorem 4) and

$$F_s(\varphi^x_{A_1\cdots A_M}) = \max_{\left\{|\phi^{x,i}\rangle_{A_i}\right\}_{i=1}^M} \left|\langle\varphi^x|_{A_1\cdots A_M}|\phi^{x,1}\rangle_{A_1} \otimes \cdots \otimes |\phi^{x,M}\rangle_{A_M}\right|^2. \tag{94}$$

For the multipartite case of the distributed quantum computation, the verifier prepares a purification $\psi^\rho_{RA_1\cdots A_M}$ of $\rho_{A_1\cdots A_M}$. The prover applies a multipartite entanglement-breaking channel on system R, which can be written as

$$\mathcal{E}_{R\to A'_1\cdots A'_{M-1}}(\cdot) = \sum_x \text{Tr}[\mu_R^x(\cdot)] \left(\phi_{A'_1}^{x,1} \otimes \cdots \otimes \phi_{A'_{M-1}}^{x,M-1}\right), \tag{95}$$

where $\{\mu_R^x\}_x$ is a rank-one POVM and $\{\phi_{A'_i}^{x,i}\}_{x,i}$ is a set of pure states. The prover sends systems $(A^{M-1})' \equiv A'_1\cdots A'_{M-1}$ to the verifier. Now, the verifier performs a collective swap test of these systems with $A_1\cdots A_M$, as depicted in Figure 11. The acceptance probability of this distributed quantum computation is given by

$$\max_{\mathcal{E}\in\text{EB}_{M-1}} \text{Tr}[\Pi^{\text{sym}}_{(A^{M-1})'A^{M-1}} \mathcal{E}_{R\to(A^{M-1})'}(\psi_{RA^{M-1}})], \tag{96}$$

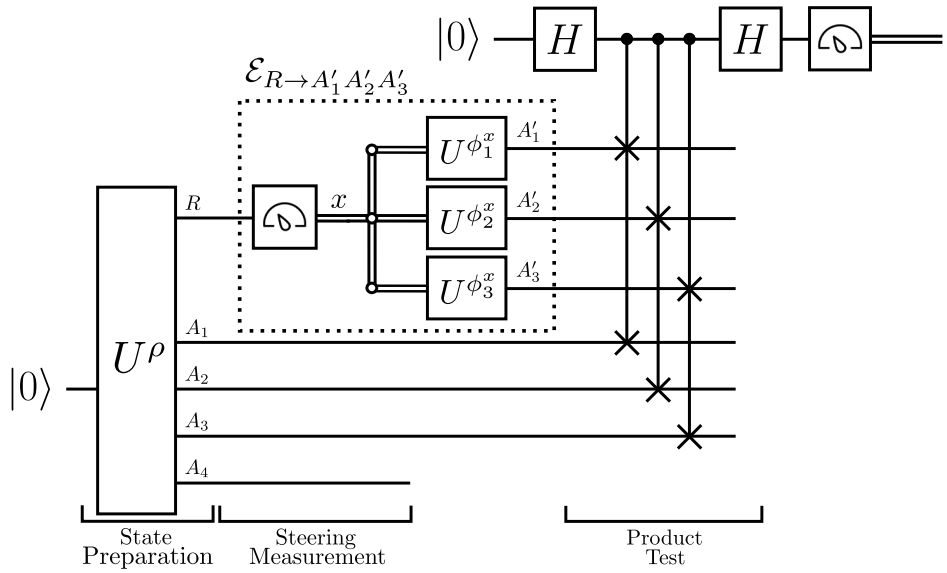


Figure 11: Test for separability of multipartite mixed states. The verifier uses a unitary circuit U^ρ to produce the state $\psi_{RA_1A_2A_3A_4}$, which is a purification of $\rho_{A_1A_2A_3A_4}$. The prover (indicated by the dotted box) applies an entanglement-breaking channel $\mathcal{E}_{R\to A_1'A_2'A_3'}$ on R by measuring the rank-one POVM $\{\mu_R^x\}_x$ and then, depending on the outcome x, prepares a state from the set $\{\phi_{A_1'}^{x,1}\otimes\phi_{A_2'}^{x,2}\otimes\phi_{A_3'}^{x,3}\}_x$. The final state is sent to the verifier, who performs a collective swap test. Theorem 10 states that the maximum acceptance probability of this interactive proof is equal to $\frac{1}{2}(1+F_s(\rho_{A_1A_2A_3A_4}))$, i.e., a simple function of the multipartite fidelity of separability.

where $\mathcal{E}\in\mathrm{EB}_{M-1}$ denotes the set of entanglement-breaking channels defined in (95). This leads to the following theorem:

Theorem 10 *For a pure state $\psi_{RA^M}\equiv\psi_{RA_1\cdots A_M}$, the following equality holds:*

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}}\mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'(A^{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA^M})]=\frac{1}{2}\left(1+\max_{\sigma_{A_1\cdots A_M}\in M-\mathrm{SEP}}F(\rho_{A_1\cdots A_M},\sigma_{A_1\cdots A_M})\right). \tag{97}$$

Proof. The circuit diagram is given in Figure 11. The verifier prepares a purification $\psi^\rho_{RA_1\cdots A_M}$ of $\rho_{A_1\cdots A_M}$. The prover applies a multipartite entanglement-breaking channel on R, which can be written as

$$\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\cdot)=\sum_x\mathrm{Tr}[\mu_R^x(\cdot)]\left(\phi_{A_1'}^{x,1}\otimes\cdots\otimes\phi_{A_{M-1}'}^{x,M-1}\right), \tag{98}$$

where $\{\mu_R^x\}_x$ is a rank-one POVM and $\{\phi_{A_i'}^{x,i}\}_{x,i}$ is a set of pure states. The prover sends the systems $(A^{M-1})'=A_1'\cdots A_{M-1}'$ to the verifier. Now, the verifier performs a collective swap test on $A_1\cdots A_M$, as depicted at the final part of the circuit diagram in Figure 11. The acceptance probability of this interactive proof system is thus given by

$$\max_{\mathcal{E}\in\mathrm{EB}}\mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}\mathcal{E}_{R\to(A_1\cdots A_{M-1})'}(\psi_{RA_1\cdots A_M})], \tag{99}$$

where

$$\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}:=\frac{1}{2}\left(I_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}+F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}\right) \tag{100}$$

is the projector onto the symmetric subspace of A' and A and $F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}$ is a tensor product of individual swaps $F_{A_i'A_i}$, for $i \in \{1,\ldots,M\}$. That is,

$$F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} = \bigotimes_{i=1}^{n} F_{A_i'A_i}. \tag{101}$$

Then we find, for fixed $\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}$, that

$$\begin{aligned}
&\operatorname{Tr}[\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA_1\cdots A_M})] \\
&= \frac{1}{2}\operatorname{Tr}[(I_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})} + F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})})\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA_1\cdots A_M})] && (102)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA^M})] && (103)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}\left[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\sum_x \operatorname{Tr}[\mu_R^x(\psi_{RA^M})]\phi^{x,1}_{A_1'}\otimes\cdots\otimes\phi^{x,M-1}_{A_{M-1}'}\right], && (104)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}\left[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\sum_x p(x)(\psi^x_{A_1\cdots A_M})\phi^{x,1}_{A_1'}\otimes\cdots\otimes\phi^{x,M-1}_{A_{M-1}'}\right], && (105)\\
&= \frac{1}{2} + \frac{1}{2}\sum_x p(x)\operatorname{Tr}\left[\left(\phi^{x,1}_{A_1}\otimes\cdots\otimes\phi^{x,M-1}_{A_{M-1}}\right)\psi^x_{A_1\cdots A_{M-1}}\right], && (106)
\end{aligned}$$

where

$$p(x) \coloneqq \operatorname{Tr}[\mu_R^x\psi_{RA^M}], \tag{107}$$

$$\psi^x_{A_1\cdots A_M} \coloneqq \frac{1}{p(x)}\operatorname{Tr}_R[\mu_R^x\psi_{RA^M}]. \tag{108}$$

For a given x, let us simplify $F_s(\varphi_{A_1\cdots A_M})$ as defined in (94),

$$\begin{aligned}
F_s(\varphi_{A_1\cdots A_M}) &= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^M} \left|\langle\varphi|_{A_1\cdots A_M}|\phi^1\rangle_{A_1}\otimes\cdots\otimes|\phi^M\rangle_{A_M}\right|^2 && (109)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^M} \left|\langle\phi^1|_{A_1}\otimes\cdots\otimes\langle\phi^M|_{A_M}|\varphi\rangle_{A_1\cdots A_M}\right|^2 && (110)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \left\|\langle\phi^1|_{A_1}\otimes\cdots\otimes\langle\phi^{M-1}|_{A_{M-1}}\otimes I_{A_M}|\varphi\rangle_{A^M}\right\|_2^2 && (111)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \operatorname{Tr}[(|\phi^1\rangle\langle\phi^1|_{A_1}\otimes\cdots\otimes|\phi^{M-1}\rangle\langle\phi^{M-1}|_{A_{M-1}}\otimes I_{A_M})\varphi_{A_1\cdots A_M}] && (112)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \operatorname{Tr}[(|\phi^1\rangle\langle\phi^1|_{A_1}\otimes\cdots\otimes|\phi^{M-1}\rangle\langle\phi^{M-1}|_{A_{M-1}})\varphi_{A_1\cdots A_{M-1}}]. && (113)
\end{aligned}$$

The first two equalities are from the definition and a rewriting. The third equality follows from the variational characterization of the Euclidean norm of a vector. Noting the form in (113) and applying the maximization over entanglement-breaking channels of the form described in (95) to (106), we arrive at the desired claim in (97). ■

We can then use the generalized test of separability of mixed states to develop a VQSA for the multipartite case. See Figure 12. This involves replacing the collective swap test in Figure 11 with an overlap measurement, similar to how we got Figure 2 in the main text from Figure 1 in the main text.

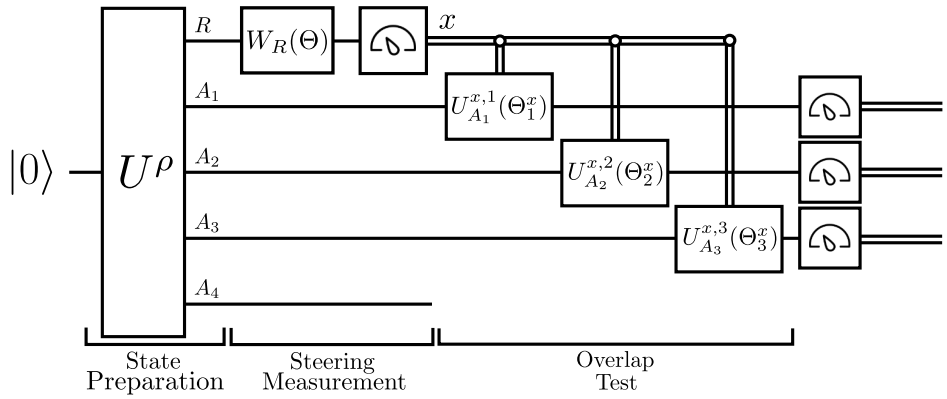


Figure 12: VQSA to estimate the multipartite fidelity of separability $F_s(\rho_{A_1A_2A_3A_4})$. The unitary circuit U^ρ prepares the state $\psi_{RA_1A_2A_3A_4}$, which is a purification of $\rho_{A_1A_2A_3A_4}$. The parameterized circuit $W_R(\Theta)$ acts on R to evolve the state to another purification of $\rho_{A_1A_2A_3A_4}$. The following measurement, labeled "steering measurement," steers the remaining systems to be in a state $\psi^x_{A_1A_2A_3A_4}$ if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuits $U^{x,1}_{A_1}(\Theta^x_1)$, $U^{x,2}_{A_2}(\Theta^x_2)$, and $U^{x,3}_{A_3}(\Theta^x_3)$ are applied and the subsequent measurement estimates the quantity $\mathrm{Tr}\left[\left(\phi^{x,1}_{A_1}\otimes\phi^{x,2}_{A_2}\otimes\phi^{x,3}_{A_3}\right)\psi^x_{A_1A_2A_3}\right]$.

J Complexity Class $\mathrm{QIP}_{\mathrm{EB}}(2)$

In this appendix, we establish a complete problem for $\mathrm{QIP}_{\mathrm{EB}}(2)$, and then we interpret this problem in Remark 13. See [41, 42] for further background on quantum computational complexity theory. Let us first define the complexity class $\mathrm{QIP}_{\mathrm{EB}}(2)$. Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a promise problem, and let $a, b : \mathbb{N} \to [0,1]$ and p be polynomial functions. The verifier V is described by a polynomial-time generated family of quantum circuits. The prover P is a family of arbitrary entanglement-breaking channels that interface with a given verifier naturally. Then $A \in \mathrm{QIP}_{\mathrm{EB}}(2)(a,b)$ if there exists a two-message verifier with the following properties:

1. Completeness: For all $x \in A_{\mathrm{yes}}$, there exists a prover P that causes the verifier V to accept x with probability at least $a(|x|)$.
2. Soundness: For all $x \in A_{\mathrm{no}}$, every prover P causes the verifier V to accept x with probability at most $b(|x|)$.

In the above, acceptance is defined as obtaining the outcome one upon measuring the decision-qubit register.

Problem 11 *Given are circuits to generate a channel $\mathcal{N}_{G\to S}$ and a state ρ_S. Fix α and β such that $0 \leq \alpha < \beta \leq 1$. Decide which of the following holds:*

$$\textit{Yes:}\quad f(\mathcal{N}_{G\to S}, \rho_S) \geq \beta, \tag{114}$$

$$\textit{No:}\quad f(\mathcal{N}_{G\to S}, \rho_S) \leq \alpha, \tag{115}$$

where

$$f(\mathcal{N}_{G\to S}, \rho_S) := \max_{\{(p(x),\psi^x)\}_x, \{\varphi^x\}_x} \left\{ \sum_x p(x) F(\psi^x_S, \mathcal{N}_{G\to S}(\varphi^x_G)) : \sum_x p(x)\psi^x_S = \rho_S \right\} \tag{116}$$

with the optimization being over every pure-state decomposition of ρ_S as $\sum_x p(x)\psi^x_S = \rho_S$. Also, $\{\varphi^x\}_x$ is a set of pure states.

Theorem 12 *Problem 11 is a complete problem for* $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Proof. The main idea behind the proof is to show that the acceptance probability of a general $\mathrm{QIP}_{\mathrm{EB}}(2)$ problem can precisely be written as $f(\mathcal{N}_{G\to S}, \rho_S)$. This implies that an arbitrary $\mathrm{QIP}_{\mathrm{EB}}(2)$ problem can be reduced to an instance of Problem 11, and we argue at the end how this also implies that Problem 11 can be reduced to an instance of a problem in $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Consider a general interactive proof system in $\mathrm{QIP}_{\mathrm{EB}}(2)$ that begins with the verifier preparing a bipartite pure state ψ_{RS}, followed by the system R being sent to the prover, which subsequently performs an entanglement-breaking channel. The verifier then performs a unitary $V_{R'S\to DG}$ and projects onto the $|1\rangle\langle 1|$ state of the decision qubit. Indeed, the acceptance probability is given by

$$\max_{\mathcal{E}\in\mathrm{EB}} \mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}_{R'S\to DG}(\mathcal{E}_{R\to R'}(\psi_{RS}))], \tag{117}$$

where $\mathcal{V}_{R'S\to DG}$ is the unitary channel corresponding to the unitary operator $V_{R'S\to DG}$. By the reasoning similar to that in (25), (32), and (33), we find that

$$\mathcal{E}_{R\to R'}(\psi_{RS}) = \sum_x p(x)\phi^x_{R'} \otimes \psi^x_S, \tag{118}$$

so that the acceptance probability is equal to

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\\ \sum_x p(x)\psi^x_S=\psi_S}} \mathrm{Tr}\left[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\left(\sum_x p(x)\phi^x_{R'} \otimes \psi^x_S\right)\right]$$

$$= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\\ \sum_x p(x)\psi^x_S=\psi_S}} \sum_x p(x)\,\mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\left(\phi^x_{R'} \otimes \psi^x_S\right)], \tag{119}$$

where we have used the shorthand $\mathcal{V} \equiv \mathcal{V}_{R'S\to DG}$. Consider that

$$\mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\left(\phi^x_{R'} \otimes \psi^x_S\right)] = \|\langle 1|_D \otimes I_G)V|\phi^x\rangle_{R'} \otimes |\psi^x\rangle_S\|_2^2 \tag{120}$$

$$= \max_{|\varphi^x\rangle_G} |\langle 1|_D \otimes \langle\varphi^x|_G)V|\phi^x\rangle_{R'} \otimes |\psi^x\rangle_S|^2 \tag{121}$$

$$= \max_{|\varphi^x\rangle_G} \mathrm{Tr}\left[V^\dagger(|1\rangle\langle 1|_D \otimes |\varphi^x\rangle\langle\varphi^x|_G)V\phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S\right] \tag{122}$$

$$= \max_{|\varphi^x\rangle_G} \mathrm{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G)\phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S], \tag{123}$$

where the isometric channel $\mathcal{W}_{G\to R'S}$ is defined as

$$\mathcal{W}_{G\to R'S}(\cdot) \coloneqq (V_{R'S\to DG})^\dagger(|1\rangle\langle 1|_D \otimes (\cdot)_G)V_{R'S\to DG}. \tag{124}$$

Then, the acceptance probability is given by

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\{\varphi^x\}_x}} \left\{ \begin{array}{c} \sum_x p(x)\,\mathrm{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G)\phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S] : \\ \sum_x p(x)\psi^x_S = \psi_S \end{array} \right\}. \tag{125}$$

Since the optimization over $\phi^x_{R'}$ is arbitrary, we can also write

$$\max_{|\phi^x\rangle_{R'}} \mathrm{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G)\phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S]$$

$$= \max_{|\phi^x\rangle_{R'}} |\langle\phi^x|_{R'} \otimes \langle\psi^x|_S W_{G\to R'S}|\varphi^x\rangle_G|^2 \tag{126}$$

$$= \|I_{R'} \otimes \langle\psi^x|_S W_{G\to R'S}|\varphi^x\rangle_G\|_2^2 \tag{127}$$

$$= \left(\langle\varphi^x|_G \left(W_{G\to R'S}\right)^\dagger I_{R'} \otimes |\psi^x\rangle_S\right)\left(I_{R'} \otimes \langle\psi^x|_S W_{G\to R'S}|\varphi^x\rangle_G\right) \tag{128}$$

$$= \langle\varphi^x|_G \left(W_{G\to R'S}\right)^\dagger \left(I_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S\right) W_{G\to R'S}|\varphi^x\rangle_G \tag{129}$$

$$= \mathrm{Tr}\Big[\left(I_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S\right) W_{G\to R'S}|\varphi^x\rangle\langle\varphi^x|_G \left(W_{G\to R'S}\right)^\dagger\Big] \tag{130}$$

$$= \mathrm{Tr}[|\psi^x\rangle\langle\psi^x|_S \mathcal{N}_{G\to S}(|\varphi^x\rangle\langle\varphi^x|_G)], \tag{131}$$

where we define the channel $\mathcal{N}_{G\to S}$ as

$$\mathcal{N}_{G\to S}(\cdot) \coloneqq \mathrm{Tr}_{R'}[(V_{R'S\to DG})^\dagger(|1\rangle\langle 1|_D \otimes (\cdot)_G) V_{R'S\to DG}]. \tag{132}$$

Then, we find that the acceptance probability is given by

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x = \psi_S}} \sum_x p(x)\,\mathrm{Tr}[|\psi^x\rangle\langle\psi^x|_S \mathcal{N}_{G\to S}(|\varphi^x\rangle\langle\varphi^x|_G)] = \max_{\substack{\{(p(x),\psi^x)\}_x, \{\varphi^x\}_x\\ \sum_x p(x)\psi_S^x = \psi_S}} \sum_x p(x) F(\psi_S^x, \mathcal{N}_{G\to S}(\varphi_G^x)). \tag{133}$$

This concludes the proof of the first part.

To see how this implies that Problem 11 can be realized in $\mathrm{QIP}_{\mathrm{EB}}(2)$, note that the circuit preparing the state ρ_S prepares a purification and traces over the reference system, and the circuit to generate $\mathcal{N}_{G\to S}$ is realize by adjoining an environment system in the state $|0\rangle\langle 0|$, performing a unitary, and tracing over the environment. So we let the verifier prepare the purification of ρ_S and this plays the role of ψ_{RS} above, and the channel $\mathcal{N}_{G\to S}$ can be realized precisely as in (132) with appropriate substitutions. ■

Remark 13 *The quantity in (116) can be interpreted as follows: Given a channel $\mathcal{N}$ and a source state ρ, calculate the largest average ensemble fidelity attainable in reproducing the source at the output of the channel. This means it is necessary to find the ensemble decomposition $\{(p(x),\psi^x)\}_x$ of ρ as well as a set $\{\varphi^x\}_x$ of encoding states that lead to the largest ensemble fidelity (and this is what is left to the prover). This criterion is similar to one used in Schumacher data compression [90], but this seems more similar to the setting of the source-channel separation theorem [91], in which the goal is to transmit an information source over a quantum channel. The channel $\mathcal{N}$ here could consist of a fixed encoding $\mathcal{E}$, noisy channel $\mathcal{M}$, and fixed decoding $\mathcal{D}$, (i.e., $\mathcal{N} = \mathcal{D}\circ\mathcal{M}\circ\mathcal{E}$) and then the goal is to test how well a given fixed scheme $(\mathcal{E},\mathcal{D})$ can communicate a source ρ over a channel $\mathcal{M}$, according to the ensemble fidelity criterion.*

Remark 14 *We can write the expression in (116) alternatively as*

$$\text{Eq. (116)} = \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \sum_x p(x)\psi_S^x = \rho_S}} \sum_x p(x) \left\|(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\right\|_\infty, \tag{134}$$

where $(\mathcal{N}_{G\to S})^\dagger$ is the Hilbert–Schmidt adjoint of the channel $(\mathcal{N}_{G\to S})^\dagger$. Employing the abbreviations $\psi_S^x \equiv |\psi^x\rangle\langle\psi^x|_S$ and $\varphi_G^x \equiv |\varphi^x\rangle\langle\varphi^x|_G$, this follows because

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x = \psi_S}} \sum_x p(x)\,\mathrm{Tr}[\psi_S^x \mathcal{N}_{G\to S}(\varphi_G^x)]$$

$$= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x) \operatorname{Tr}[(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\varphi_G^x] \tag{135}$$

$$= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x) \max_{\{\varphi^x\}_x} \operatorname{Tr}[(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\varphi_G^x] \tag{136}$$

$$= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \sum_x p(x)\psi_S^x=\rho_S}} \sum_x p(x) \left\|(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\right\|_\infty . \tag{137}$$

If we define the function

$$g_{\mathcal{N}}(\rho) := \left\|(\mathcal{N}_{G\to S})^\dagger(\rho_S)\right\|_\infty , \tag{138}$$

then the function in (134) is known as the concave closure of $g_{\mathcal{N}}(\rho)$ and has been studied in other contexts in quantum information theory [92, Section 2]. It has an interesting dual formulation, as demonstrated in [92, Eq. (15)]. Given the observation in (134), we can thus conclude that, given circuits to realize the channel $\mathcal{N}$ and state ρ, estimating the concave closure of the function $g_{\mathcal{N}}(\rho)$ within additive error is a complete problem for $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Remark 15 *Employing the reasoning from Remark 14, we find that the acceptance probability in (35) is equal to the concave closure of the following function:*

$$f(\rho_{AB}) := \|\Pi_{AA'}^{\mathrm{sym}}(\rho_{AB}\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}\|_\infty , \tag{139}$$

where we used the fact that the state ρ_S from Remark 14 is ρ_{AB} and the map $\mathcal{N}_{G\to S}$ from Remark 14 is

$$\mathcal{N}(\sigma_{AA'B}) = \operatorname{Tr}_{A'}[\Pi_{AA'}^{\mathrm{sym}}\sigma_{AA'B}\Pi_{AA'}^{\mathrm{sym}}], \tag{140}$$

with adjoint

$$\mathcal{N}^\dagger(\omega_{AB}) = \Pi_{AA'}^{\mathrm{sym}}(\omega_{AB}\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}. \tag{141}$$

Observe that the map $\rho_{AB}\mapsto \Pi_{AA'}^{\mathrm{sym}}(\rho_{AB}\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}$ is proportional to that used in a $1\to 2$ universal cloning machine [93, Eq. (17)]. If ρ_{AB} is pure, so that we write it as ψ_{AB}, then the following inequality holds:

$$\|\Pi_{AA'}^{\mathrm{sym}}(\psi_{AB}\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}\|_\infty \leq \|\Pi_{AA'}^{\mathrm{sym}}\|_\infty \|\psi_{AB}\otimes I_{A'}\|_\infty \|\Pi_{AA'}^{\mathrm{sym}}\|_\infty \leq 1, \tag{142}$$

where we applied the multiplicativity of the spectral norm. Thus, the concave closure of $f(\rho_{AB})$ satisfies $f(\rho_{AB})\in[0,1]$. Furthermore, from Lemma 16 below, we know that

$$\|\Pi_{AA'}^{\mathrm{sym}}(\psi_{AB}\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}\|_\infty = \frac{1}{2}\left(1+\|\psi_A\|_\infty\right), \tag{143}$$

showing the consistency of the claim just above (139) with Theorem 1 and Eqs. (19) and (20) in the main text. If ρ_{AB} is a pure product state, so that we can write it as $\rho_{AB}=\phi_A\otimes\varphi_B$, then we have that

$$\|\Pi_{AA'}^{\mathrm{sym}}(\phi_A\otimes\varphi_B\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}\|_\infty = \|\Pi_{AA'}^{\mathrm{sym}}(\phi_A\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}\|_\infty , \tag{144}$$

and the spectral norm on the right-hand side of (144) is achieved by choosing the vector $|\phi\rangle_A\otimes|\phi\rangle_{A'}$, so that

$$(\langle\phi|_A\otimes\langle\phi|_{A'})\Pi_{AA'}^{\mathrm{sym}}(\phi_A\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}(|\phi\rangle_A\otimes|\phi\rangle_{A'})$$

$$= (\langle\phi|_A\otimes\langle\phi|_{A'})(\phi_A\otimes I_{A'})(|\phi\rangle_A\otimes|\phi\rangle_{A'}) \tag{145}$$

$$= 1. \tag{146}$$

Lemma 16 *For a pure state ψ_{AB}, the following equality holds:*

$$\|\Pi^{\mathrm{sym}}_{AA'}(\psi_{AB}\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\|_\infty = \frac{1}{2}\left(1+\|\psi_A\|_\infty\right), \tag{147}$$

where $\psi_A \equiv \mathrm{Tr}_B[\psi_{AB}]$.

Proof. Consider that

$$\begin{aligned}\|(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B)\|_\infty \\ = \|(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\left(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B\right)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\|_\infty .\end{aligned} \tag{148}$$

Now consider that

$$\begin{aligned}&(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\left(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B\right)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\\ &= (|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\left(\frac{I_{AA'}+F_{AA'}}{2}\otimes I_B\right)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}) &(149)\\ &= \frac{1}{2}(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}) + \frac{1}{2}(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})(F_{AA'}\otimes I_B)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}). &(150)\end{aligned}$$

Then writing the Schmidt decomposition of $|\psi\rangle_{AB}$ as $|\psi\rangle_{AB}=\sum_i\sqrt{\lambda_i}|i\rangle_A|i\rangle_B$, we find that

$$\begin{aligned}&(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})(F_{AA'}\otimes I_B)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\\ &= \sum_{i,i',j,j'}\sqrt{\lambda_i\lambda_{i'}}(|\psi\rangle\langle i|_A\langle i|_B\otimes|j\rangle\langle j|_{A'})(F_{AA'}\otimes I_B)(|i'\rangle_A|i'\rangle_B\langle\psi|_{AB}\otimes|j'\rangle\langle j'|_{A'}) &(151)\\ &= \sum_{i,i',j,j'}\sqrt{\lambda_i\lambda_{i'}}(|\psi\rangle\langle i|_A\langle i|_B\otimes|j\rangle\langle j|_{A'})(|j'\rangle_A|i'\rangle_B\langle\psi|_{AB}\otimes|i'\rangle\langle j'|_{A'}) &(152)\\ &= \sum_{i,i',j,j'}\sqrt{\lambda_i\lambda_{i'}}|\psi\rangle\langle i|j'\rangle_A\langle i|i'\rangle_B\langle\psi|_{AB}\otimes|j\rangle\langle j|i'\rangle\langle j'|_{A'} &(153)\\ &= \sum_i\lambda_i|\psi\rangle\langle\psi|_{AB}\otimes|i\rangle\langle i|_{A'} &(154)\\ &= |\psi\rangle\langle\psi|_{AB}\otimes\sum_i\lambda_i|i\rangle\langle i|_{A'} &(155)\\ &= |\psi\rangle\langle\psi|_{AB}\otimes\psi_{A'}. &(156)\end{aligned}$$

Then

$$\begin{aligned}&(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})\\ &= \frac{1}{2}(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}) + |\psi\rangle\langle\psi|_{AB}\otimes\frac{1}{2}\psi_{A'} &(157)\\ &= |\psi\rangle\langle\psi|_{AB}\otimes\frac{1}{2}(I_{A'}+\psi_{A'}), &(158)\end{aligned}$$

and we conclude that

$$\begin{aligned}&\|(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B)(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'})(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B)\|_\infty\\ &= \left\||\psi\rangle\langle\psi|_{AB}\otimes\frac{1}{2}(I_{A'}+\psi_{A'})\right\|_\infty &(159)\\ &= \frac{1}{2}(1+\|\psi_{A'}\|_\infty) &(160)\end{aligned}$$

$$= \frac{1}{2}\left(1 + \|\psi_A\|_\infty\right). \tag{161}$$

This concludes the proof. ■

K Placement of $\mathsf{QIP}_{\mathrm{EB}}(2)$

In this appendix, we establish the following containments:

$$\mathrm{QAM}, \mathrm{QSZK} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2). \tag{162}$$

See Figure 7 for a detailed diagram.

K.1 $\mathsf{QAM} \subseteq \mathsf{QIP}_{\mathrm{EB}}(2)$

First, recall that QAM consists of the verifier selecting a classical letter x uniformly at random, sending the choice to the prover, who then sends back a pure state ψ_x to the verifier, who finally performs an efficient measurement to decide whether to accept the computation [55]. Note that QAM contains QMA [55].

To see the containment $\mathrm{QAM} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2)$, consider that the verifier's first circuit in $\mathrm{QIP}_{\mathrm{EB}}(2)$ can consist of preparing a random classical bitstring in a system R. The verifier sends system R to the prover. Then, the prover's action amounts to preparing some state that gets returned to the verifier. The rest of the protocol then simulates a QAM protocol.

K.2 $\mathsf{QSZK} \subseteq \mathsf{QIP}_{\mathrm{EB}}(2)$

Quantum statistical zero-knowledge (QSZK) consists of all problems that can be solved by the interaction between a quantum verifier and a quantum prover, such that the verifier accumulates statistical evidence about the answer to a decision, but does not learn anything other than the answer by interacting with the prover [94, 56]. A complete problem for this class is quantum state distinguishability, in which the goal is to decide whether two states ρ_0 and ρ_1, generated by quantum circuits, are far or close in trace distance [94]. This is a nice problem for understanding the basics of the QSZK complexity class: the interaction begins with the verifier picking one of the states uniformly at random, recording the choice as a bit x, and then sending the chosen state ρ_x to the prover over a quantum channel. The prover can then perform the optimal Helstrom measurement [95, 96] to distinguish the states which has success probability equal to

$$p_{\mathrm{succ}} \coloneqq \frac{1}{2}\left(1 + \frac{1}{2}\left\|\rho_0 - \rho_1\right\|_1\right). \tag{163}$$

The Helstrom measurement leads to a decision bit y, which the prover sends back to the verifier over a quantum channel (here, a single classical bit channel would suffice). The verifier then accepts if $x = y$, and the probability that this happens is equal to p_{succ}. By repeating this protocol a polynomial number of times and invoking the error-reduction protocol from [94], it follows that the verifier can make the completeness and soundness probabilities exponentially close to one and zero, respectively, to have essentially zero error probability in the final decision about whether the states are near or far in trace distance. Finally, the interaction has a "zero knowledge" aspect because the verifier only learns the bit of the prover and nothing about how to distinguish the states.

Since quantum state distinguishability is a complete problem for QSZK and the interaction described above can be performed in $\mathrm{QIP}_{\mathrm{EB}}(2)$, $\mathrm{QSZK} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2)$follows.

L Local Reward Function

In this appendix, we develop a local reward function as an alternative to the global reward function considered in the main text, i.e., the acceptance probability in Theorem 2. The acceptance probability in Theorem 2 can be considered a global reward function because it corresponds to the probability of measuring zero in every register. As indicated in [44], it is helpful to employ a local reward function to mitigate the barren plateau problem [43], which plagues all variational quantum algorithms.

Let us define the local and global reward functions. Let Z_i be the event of measuring zero in the ith register. We then set the local reward function to be the probability of measuring zero in a register chosen uniformly at random; that is, it is given by the following:

$$L \equiv \frac{1}{n} \sum_i \Pr(Z_i) \,. \tag{164}$$

The event of measuring all zeros is given by $\bigcap_i Z_i$, and the probability that this event occurs is $G \equiv \Pr(\bigcap_i Z_i)$, which is what we used in the main text as the global reward function.

We are interested in determining inequalities related to the global and local reward functions, and the following analysis employs the same ideas used in [81, Appendix C]. Using DeMorgan's laws, we find that

$$\Pr\left(\bigcap_i Z_i\right) = \Pr\left(\left(\bigcup_i Z_i^c\right)^c\right) = 1 - \Pr\left(\bigcup_i Z_i^c\right). \tag{165}$$

We can then use the union bound to conclude that

$$\Pr\left(\bigcap_i Z_i\right) = 1 - \Pr\left(\bigcup_i (Z_i)^c\right) \geq 1 - \sum_i \Pr((Z_i)^c) \,. \tag{166}$$

Finally, consider that

$$\begin{aligned} G &= \Pr\left(\bigcap_i Z_i\right) && (167)\\ &\geq 1 - \sum_i \Pr(Z_i^c) && (168)\\ &= \sum_i \Pr(Z_i) - (n-1) && (169)\\ &= nL - (n-1) && (170)\\ &= n(L-1) + 1. && (171) \end{aligned}$$

We can also derive an upper bound on the global reward function in terms of the local reward function. Recall the following inequality, which holds for every set $\{A_1, A_2, \ldots, A_n\}$ of events:

$$\Pr\left(\bigcup_i A_i\right) \geq \frac{1}{n} \sum_i \Pr(A_i) \,. \tag{172}$$

Setting $A_i = Z_i^c$, we get

$$\Pr\left(\bigcup_i Z_i^c\right) \geq \frac{1}{n} \sum_i \Pr(Z_i^c) \,. \tag{173}$$

Using DeMorgan's laws, we obtain the desired upper bound as follows:

$$\Pr\left(\bigcap_i Z_i\right) \leq 1 - \frac{1}{n}\sum_i (1 - \Pr(Z_i)) \tag{174}$$

$$= \frac{1}{n}\sum_i \Pr(Z_i)\,. \tag{175}$$

In summary, we have established the following bounds:

$$n(L-1) + 1 \leq G \leq L, \tag{176}$$

so that $G = 1$ if and only if $L = 1$. Since we always have $G \in [0, 1]$, the lower bound is only nontrivial if L is sufficiently large, i.e., if $L \geq 1 - \frac{1}{n}$.