

One-Sided Error QMA with Shared EPR Pairs—A Simpler Proof

Attila Pereszlenyi*

Centre for Quantum Technologies, National University of Singapore

23rd June, 2013

Abstract

We give a simpler proof of one of the results of Kobayashi, Le Gall, and Nishimura [KLG13], which shows that any QMA protocol can be converted to a one-sided error protocol, in which Arthur and Merlin initially share a constant number of EPR pairs and then Merlin sends his proof to Arthur. Our protocol is similar but somewhat simpler than the original. Our main contribution is a simpler and more direct analysis of the soundness property that uses well-known results in quantum information such as properties of the trace distance and the fidelity, and the quantum de Finetti theorem.

1 Introduction

The class MA was defined by Babai [Bab85] as the natural probabilistic extension of the class NP. In the definition of MA, the prover (Merlin) gives a polynomial length ‘proof’ to the verifier (Arthur), who then performs a polynomial-time randomized computation and has to decide if an input x is in a language L or not. If we add interaction to the model, i.e., the prover and the verifier can exchange a polynomial number of messages before the verifier makes his decision, then we get the class IP [GMR89].¹ The verifiers of the above proof systems are allowed to make some small error in their decision, but they must satisfy two conditions.

- If $x \in L$ then the verifier has to accept a valid proof with high probability. The probability that the verifier rejects such proof is called the *completeness* error.
- If $x \notin L$ then no matter what proof the verifier receives, he must reject with high probability. The probability that the verifier accepts an invalid proof is called the *soundness* error.

One of the first questions one may ask is whether it is possible to get rid of one or both types of error. It is easy to see that forcing the soundness error to zero collapses IP (and also MA) to NP [AB09]. So we can’t eliminate the soundness error completely, but it is known that we can make it to be at most an inverse-exponential function of the input length, without reducing the expressive power of MA or IP. On the other hand, it was shown by Zachos and Fürer [ZF87] that having *perfect completeness*, also called as *one-sided error*, doesn’t change the power of MA. More formally, it holds that $MA = MA_1$, where MA_1 is the class with perfect completeness. The class IP can also be made to have one-sided error, which follows, for example, from the

*E-mail: attila.pereszlenyi@gmail.com.

¹Babai also defined an interactive version of MA, that can be thought of as a ‘public-coin’ version of IP. Later Goldwasser and Sipser [GS86] showed that this class has the same expressive power as IP.

characterization of IP being equal to PSPACE, the class of problems decidable in polynomial space [LFKN92, Sha92, She92]. For more information on these classes see e.g., the book of Arora and Barak [AB09].

Quantum Merlin-Arthur proof systems (and the class QMA) were introduced by Knill [Kni96], Kitaev [KSV02], and also by Watrous [Wat00] as a natural extension of MA and NP to the quantum computational setting. Similarly, quantum interactive proof systems (and the class QIP) were introduced by Watrous [Wat03] as a quantum analogue of IP. These classes have also been well studied and now it's known that the power of quantum interactive proof systems is the same as the classical ones, i.e., $\text{QIP} = \text{IP} = \text{PSPACE}$ [JJUW10]. Furthermore, quantum interactive proof systems still have the same expressive power if we restrict the number of messages to three and have exponentially small one-sided error [KW00].

The class QMA is not as well understood as QIP, but we do have a reasonable amount of knowledge about it. We know from the early results that it can be made to have exponentially small two-sided error [KSV02, AN02, MW05]. It also has natural complete problems, such as the ' k -local Hamiltonian' problem [KSV02, AN02], for $k \geq 2$ [KKR06], which can be thought of as a quantum analogue of k -SAT. With respect to the relation of QMA to classical complexity classes, we know that $\text{MA} \subseteq \text{QMA} \subseteq \text{PP}$ [MW05].² There are also interesting generalizations of QMA, such as with multiple unentangled provers [KMY03, ABD⁺09, HM10, BT09], but we will not consider them in this paper.

Interestingly, we don't know if $\text{QMA} \stackrel{?}{=} \text{QMA}_1$, i.e., whether QMA can be made to have perfect completeness. It is a long-standing open problem which was already mentioned in an early survey by Aharonov and Naveh [AN02]. Besides its inherent importance, giving a positive answer to it would immediately imply that the QMA_1 -complete problems are also complete for QMA. Most notable of these is the 'Quantum k -SAT' problem of Bravyi [Bra06], for $k \geq 3$ [GN13], which is considered as a more natural quantum generalization of k -SAT than the k -local Hamiltonian problem.³ Unfortunately, all previous techniques used to show one-sided error properties of quantum interactive proof systems require adding extra messages to the protocol [KW00, KKMV08, KLG13], so they can't be used directly in QMA. Aaronson [Aar09] gave an evidence that shows that proving $\text{QMA} = \text{QMA}_1$ may be difficult. He proved that there exists a quantum oracle relative to which $\text{QMA} \neq \text{QMA}_1$. Another difficulty with QMA, compared to MA, is that in a QMA proof system the acceptance probability can be an arbitrary irrational number. However, if certain assumptions are made about the maximum acceptance probability then QMA can be made to have one-sided error [NWZ09]. Recently, Jordan, Kobayashi, Nagaj, and Nishimura [JKNN12] showed that if Merlin's proof is classical (in which case the class is denoted by QCMA), then perfect completeness is achievable, i.e., it holds that $\text{QCMA} = \text{QCMA}_1$. In another variant of QMA, where we have multiple unentangled provers and exponentially or double-exponentially small gap, we also know that perfect completeness is achievable [Per12]. The most recent and strongest result towards proving the original QMA versus QMA_1 question is by Kobayashi, Le Gall, and Nishimura [KLG13]. They showed that we can convert a QMA proof system to have one-sided error, if we allow the prover and the verifier of the resulting QMA_1 protocol to share a constant number of EPR pairs before the prover sends the proof to the verifier. The corresponding class is denoted by $\text{QMA}_1^{\text{const-EPR}}$. With this notation, their result can be formalized as the following theorem.

Theorem 1.1 ([KLG13]). $\text{QMA} \subseteq \text{QMA}_1^{\text{const-EPR}}$.

Since sharing an EPR pair can be done by the verifier preparing it and sending half of it to the prover, the above result implies that QMA is contained in the class of languages provable by

²A slightly stronger bound of $\text{QMA} \subseteq \text{A}_0\text{PP}$ was shown by Vyalıy [Vya03].

³For a list of QMA- and QMA_1 -complete problems, see e.g., [Boo12].

one-sided error, two-message quantum interactive proof systems ($\text{QMA} \subseteq \text{QIP}_1(2)$). This is a nontrivial upper bound. Moreover, a result of Beigi, Shor, and Watrous [BSW11] implies that equality in Theorem 1.1 holds, resulting in the following characterization of QMA.

Corollary 1.2 ([KLG13]). $\text{QMA} = \text{QMA}_1^{\text{const-EPR}} = \text{QMA}^{\text{const-EPR}}$.

The *contribution of this paper* is a conceptually simpler and more direct proof of Theorem 1.1, compared to the original one by Kobayashi et al. [KLG13]. The algorithm of our verifier is also simpler, but the main difference is in the proof of its soundness. We believe that our proof helps to understand the result better and we think that it may be simplified further. The description of the idea behind our proof can be found in Section 3.1, while the complete proof is presented in Section 3.2.

Organization of the Paper

The remainder of the paper is organized as follows. Section 2 discusses the background definitions, theorems, and lemmas needed to understand our proof. The proof itself is presented in Section 3, starting with a high level description in Section 3.1, and then presenting the detailed proof in Section 3.2.

2 Preliminaries

We assume familiarity with quantum information [Wat08b] and computation [NC00]; such as quantum states, unitary operators, measurements, quantum super-operators, etc. We also assume the reader is familiar with computational complexity, both classical [AB09] and quantum [Wat08a]. The purpose of this section is to present the notations and background information (definitions, theorems) required to understand the rest of the paper. In this paper we denote the imaginary unit by ι instead of i , which we use as an index in summations, for example. When we talk about a quantum register \mathcal{R} of size k , we mean the object made up of k qubits. It has associated Hilbert space $\mathcal{R} = \mathbb{C}^{2^k}$. We always assume that some standard basis of $\mathcal{R} = \mathbb{C}^{2^k}$ have been fixed and we index those basis vectors by bit strings of length k . So the standard basis of \mathcal{R} is denoted by $\{|s\rangle : s \in \{0, 1\}^k\}$. We denote the all zero string by $\bar{0} \stackrel{\text{def}}{=} 00\dots 0$. Throughout the paper, $L(\mathcal{R})$ denotes the space of all linear mappings from \mathcal{R} to itself. The set of all density operators on \mathcal{R} is denoted by $D(\mathcal{R})$. The adjoint of $\mathbf{A} \in L(\mathcal{R})$ is denoted by \mathbf{A}^* .

Definition 2.1. The *trace norm* of $\mathbf{A} \in L(\mathcal{R})$ is defined by

$$\|\mathbf{A}\|_{\text{Tr}} \stackrel{\text{def}}{=} \text{Tr}\left(\sqrt{\mathbf{A}^* \mathbf{A}}\right),$$

and the *operator norm* of \mathbf{A} is

$$\|\mathbf{A}\|_{\infty} \stackrel{\text{def}}{=} \max\{\|\mathbf{A}|\varphi\rangle\| : |\varphi\rangle \in \mathcal{R}, \|\varphi\| = 1\}.$$

The following inequality is a special case of the Hölder Inequality for Schatten norms.

Lemma 2.2. For any Hilbert space \mathcal{H} and operators $\mathbf{A}, \mathbf{B} \in L(\mathcal{H})$, it holds that

$$|\text{Tr}(\mathbf{B}^* \mathbf{A})| \leq \|\mathbf{A}\|_{\text{Tr}} \cdot \|\mathbf{B}\|_{\infty}.$$

The following definition is used to quantify the distance between operators.

Definition 2.3. The *trace distance* between operators $\mathbf{A}, \mathbf{B} \in L(\mathcal{H})$ is defined as

$$d(\mathbf{A}, \mathbf{B}) \stackrel{\text{def}}{=} \frac{\|\mathbf{A} - \mathbf{B}\|_{\text{Tr}}}{2}.$$

If the operators represent pure quantum states, i.e., $\mathbf{A} = |\varphi\rangle\langle\varphi|$ and $\mathbf{B} = |\psi\rangle\langle\psi|$, for some $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$, for which $\|\varphi\| = \|\psi\| = 1$, then the trace distance can be more conveniently written as

$$d(|\varphi\rangle, |\psi\rangle) = \sqrt{1 - |\langle\varphi|\psi\rangle|^2}. \quad (1)$$

Another way of quantifying the similarity between density operators is by the fidelity defined below.

Definition 2.4. The *fidelity* between $\rho, \sigma \in D(\mathcal{H})$ is defined as

$$F(\rho, \sigma) \stackrel{\text{def}}{=} \|\sqrt{\rho}\sqrt{\sigma}\|_{\text{Tr}}.$$

If $\rho = |\varphi\rangle\langle\varphi|$ then the fidelity can be more conveniently written as

$$F(|\varphi\rangle\langle\varphi|, \sigma) = \sqrt{\langle\varphi|\sigma|\varphi\rangle}. \quad (2)$$

The following alternate characterization of the fidelity will be useful later.

Theorem 2.5 (Uhlmann's Theorem, see e.g., [Wat08b] for a proof). *Let $\rho, \sigma \in D(\mathcal{H})$ and \mathcal{X} be a Hilbert space such that $\dim(\mathcal{X}) \geq \dim(\mathcal{H})$. Let $|\varphi\rangle \in \mathcal{X} \otimes \mathcal{H}$ be any purification of ρ , i.e., $\text{Tr}_{\mathcal{X}}(|\varphi\rangle\langle\varphi|) = \rho$. Then*

$$F(\rho, \sigma) = \max \{ |\langle\varphi|\psi\rangle| : |\psi\rangle \in \mathcal{X} \otimes \mathcal{H}, \text{Tr}_{\mathcal{X}}(|\psi\rangle\langle\psi|) = \sigma \}.$$

We now list some properties of the trace distance.

Lemma 2.6 (triangle inequality). *For any $\mathbf{A}, \mathbf{B}, \mathbf{C} \in L(\mathcal{H})$, it holds that*

$$d(\mathbf{A}, \mathbf{B}) \leq d(\mathbf{A}, \mathbf{C}) + d(\mathbf{C}, \mathbf{B}).$$

Theorem 2.7 (Theorem 9.2 from [NC00]). *Let $\Phi : L(\mathcal{H}) \rightarrow L(\mathcal{K})$ be a quantum super-operator (a completely positive and trace preserving linear map) and let $\rho, \sigma \in D(\mathcal{H})$. Then*

$$d(\Phi(\rho), \Phi(\sigma)) \leq d(\rho, \sigma).$$

Lemma 2.8. *Let $\mathbf{A}, \mathbf{B} \in L(\mathcal{H})$. If $0 \leq \mathbf{B}$ and $\text{Tr}(\mathbf{B}) \leq \varepsilon$, for some $0 \leq \varepsilon$, then*

$$d(\mathbf{A} + \mathbf{B}, \mathbf{A}) \leq \frac{\varepsilon}{2}.$$

Proof. From the definition of the trace norm and the trace distance, together with the fact that $\sqrt{\mathbf{B}^*\mathbf{B}} = \mathbf{B}$, we get that

$$\begin{aligned} d(\mathbf{A} + \mathbf{B}, \mathbf{A}) &= \frac{\|\mathbf{A} + \mathbf{B} - \mathbf{A}\|_{\text{Tr}}}{2} \\ &= \frac{\|\mathbf{B}\|_{\text{Tr}}}{2} \\ &= \frac{\text{Tr}(\mathbf{B})}{2} \\ &\leq \frac{\varepsilon}{2}. \end{aligned} \quad \square$$

Lemma 2.9. Let $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ and $0 \leq \varepsilon < 1$. It holds that

$$d((1 - \varepsilon)\rho + \varepsilon\sigma, \rho) \leq \varepsilon.$$

Proof. Using the triangle inequality (Lemma 2.6) and Lemma 2.8, we get that

$$\begin{aligned} d((1 - \varepsilon)\rho + \varepsilon\sigma, \rho) &\leq d((1 - \varepsilon)\rho + \varepsilon\sigma, (1 - \varepsilon)\rho) + d(\rho, (1 - \varepsilon)\rho) \\ &\leq \frac{\varepsilon}{2} + \frac{\|\rho - (1 - \varepsilon)\rho\|_{\text{Tr}}}{2} \\ &= \frac{\varepsilon}{2} + \frac{\text{Tr}(\varepsilon\rho)}{2} \\ &= \varepsilon. \end{aligned} \quad \square$$

The following lemma will be used to quantify how much a projective measurement changes a state. It is a variant of Winter's gentle measurement lemma [Win99].

Lemma 2.10 (Lemma 4 from [JN12]). Let $\rho \in \mathcal{D}(\mathcal{H})$ be a density operator and $\Pi \in \mathcal{L}(\mathcal{H})$ be a projector such that $\text{Tr}(\rho\Pi) < 1$. Then

$$1 - \text{Tr}(\rho\Pi) \leq F\left(\rho, \frac{(\mathbb{1} - \Pi)\rho(\mathbb{1} - \Pi)}{\text{Tr}(\rho(\mathbb{1} - \Pi))}\right)^2.$$

The following theorem gives a relation between trace distance and fidelity.

Theorem 2.11 (Fuchs-van de Graaf Inequalities, see e.g., [Wat08b] for a proof). For any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, it holds that

$$1 - d(\rho, \sigma) \leq F(\rho, \sigma) \leq \sqrt{1 - d(\rho, \sigma)^2}.$$

The following argument has appeared before, for example in [BSW11]. We present it here as a separate lemma and include its proof for convenience.

Lemma 2.12. Let $0 \leq \varepsilon \leq 1$, $\rho \in \mathcal{D}(\mathcal{A} \otimes \mathcal{B})$, and $\sigma \in \mathcal{D}(\mathcal{B})$. If

$$d(\text{Tr}_{\mathcal{A}}(\rho), \sigma) \leq \varepsilon$$

then there exists a $\tau \in \mathcal{D}(\mathcal{A} \otimes \mathcal{B})$ for which

$$\text{Tr}_{\mathcal{A}}(\tau) = \sigma \quad \text{and} \quad d(\rho, \tau) \leq \sqrt{2\varepsilon}.$$

Proof. Let us take an auxiliary Hilbert space $\mathcal{X} \cong \mathcal{A} \otimes \mathcal{B}$ and let $|\varphi\rangle \in \mathcal{X} \otimes \mathcal{A} \otimes \mathcal{B}$ be a purification of ρ , i.e., $\text{Tr}_{\mathcal{X}}(|\varphi\rangle\langle\varphi|) = \rho$. We have that

$$\begin{aligned} 1 - \varepsilon &\leq 1 - d(\text{Tr}_{\mathcal{A}}(\rho), \sigma) \\ &\leq F(\text{Tr}_{\mathcal{A}}(\rho), \sigma) \end{aligned} \quad (3)$$

$$= \max\{|\langle\varphi|\psi\rangle| : |\psi\rangle \in \mathcal{X} \otimes \mathcal{A} \otimes \mathcal{B}, \text{Tr}_{\mathcal{X} \otimes \mathcal{A}}(|\psi\rangle\langle\psi|) = \sigma\}, \quad (4)$$

where (3) follows from Theorem 2.11 and (4) follows from Theorem 2.5. This means that there exists a $|\psi\rangle \in \mathcal{X} \otimes \mathcal{A} \otimes \mathcal{B}$, such that $1 - \varepsilon \leq |\langle\varphi|\psi\rangle|$ and $\text{Tr}_{\mathcal{X} \otimes \mathcal{A}}(|\psi\rangle\langle\psi|) = \sigma$. Let

$$\tau \stackrel{\text{def}}{=} \text{Tr}_{\mathcal{X}}(|\psi\rangle\langle\psi|).$$

We only need to bound the distance between ρ and τ .

$$d(\rho, \tau) \leq d(|\phi\rangle, |\psi\rangle) \quad (5)$$

$$\begin{aligned} &= \sqrt{1 - |\langle \phi | \psi \rangle|^2} \\ &\leq \sqrt{1 - (1 - \varepsilon)^2} \\ &\leq \sqrt{2\varepsilon}, \end{aligned} \quad (6)$$

where (5) follows from Theorem 2.7 and (6) follows from (1). \square

Throughout the paper we denote the identity operator on some Hilbert space \mathcal{H} by $\mathbb{1}_{\mathcal{H}}$ and we sometimes omit the subscript if it is clear from the context. We also use some well-known unitary operators (also called quantum gates), such as the controlled-NOT (**CNOT**) gate, the Hadamard gate (**H**), and the Pauli operators (**X**, **Z**, **Y**). The definition of these operators can be found in any standard quantum textbook, for example in [NC00]. A key to our main algorithm will be the following operator which will be used to reduce the acceptance probability of a QMA verifier to $1/2$. The details will be explained later, but it is convenient to define the operator here. Let $q \in [0, 1]$, then

$$\mathbf{W}_q \stackrel{\text{def}}{=} \begin{bmatrix} \sqrt{1-q} & -i\sqrt{q} \\ -i\sqrt{q} & \sqrt{1-q} \end{bmatrix}.$$

Note that \mathbf{W}_q corresponds to a rotation about the \hat{x} axes in the Bloch sphere and it is very similar to the corresponding operator in [KLG13].

We will use the following quantum states often so it is convenient to introduce notations for them. Let

$$|\phi^+\rangle \stackrel{\text{def}}{=} \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |\phi^-\rangle \stackrel{\text{def}}{=} \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad |\phi^+\rangle, |\phi^-\rangle \in \mathbb{C}^2.$$

Note that $|\phi^+\rangle$ and $|\phi^-\rangle$ can be obtained by applying **H** on $|0\rangle$ and $|1\rangle$. We will also use the Bell basis.

Definition 2.13. The following states form a basis of \mathbb{C}^4 and are called the *Bell basis*.

$$\begin{aligned} |\Phi^+\rangle &\stackrel{\text{def}}{=} \frac{|00\rangle + |11\rangle}{\sqrt{2}}, & |\Phi^-\rangle &\stackrel{\text{def}}{=} \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ |\Psi^+\rangle &\stackrel{\text{def}}{=} \frac{|01\rangle + |10\rangle}{\sqrt{2}}, & |\Psi^-\rangle &\stackrel{\text{def}}{=} \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned}$$

The following theorem is used to eliminate the entanglement between registers.

Theorem 2.14 (quantum de Finetti theorem [CKMR07]; this form is from [Wat08b]⁴). *Let X_1, \dots, X_N be identical quantum registers, each having associated space \mathbb{C}^2 , and let $\rho \in \mathcal{D}(\mathbb{C}^{2N})$ be the state of these registers. Suppose that ρ is invariant under the permutation of the registers. Then there exist a number $m \in \mathbb{Z}^+$, a probability distribution $\{p_i : i \in \{1, 2, \dots, m\}\}$, and a collection of density operators $\{\xi_i : i \in \{1, 2, \dots, m\}\} \subset \mathcal{D}(\mathbb{C}^2)$ such that*

$$\left\| \text{Tr}_{X_3, \dots, X_N}(\rho) - \sum_{i=1}^m p_i \xi_i \otimes \xi_i \right\|_{\text{Tr}} < \frac{32}{N}.$$

⁴Note that this is not the general form of the theorem, but this simplified version will be sufficient for our proof.

Later we will use the SWAP Test of [BBD⁺97, BCWdW01] and the following property of this test.

Theorem 2.15 ([BCWdW01, KMY03]). *When the SWAP Test is applied to $\rho \otimes \sigma$, where $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, it succeeds with probability*

$$\frac{1 + \text{Tr}(\rho\sigma)}{2}.$$

In order to perform the SWAP Test, we need two Hadamard gates, $O(\log(\dim(\mathcal{H})))$ -number of CNOT gates, and we need to measure a qubit in the standard basis.

The following lemma will be the basic building block to prove perfect completeness, similarly to [KLG13].

Lemma 2.16. *Let $\Delta, \Pi \in L(\mathcal{H})$ be projectors. Suppose that one of the eigenvalues of $\Delta\Pi\Delta$ is $1/2$ with corresponding eigenstate $|\omega\rangle$. Then*

$$\Delta(\mathbb{1} - 2\Pi)\Delta|\omega\rangle = 0.$$

Proof. Using the fact that $\Delta|\omega\rangle = |\omega\rangle$, we get

$$\begin{aligned} \Delta(\mathbb{1} - 2\Pi)\Delta|\omega\rangle &= (\Delta - 2\Delta\Pi\Delta)|\omega\rangle \\ &= |\omega\rangle - 2\left(\frac{1}{2}|\omega\rangle\right) \\ &= 0. \end{aligned} \quad \square$$

In [KLG13], the procedure defined by applying $\Delta(\mathbb{1} - 2\Pi)\Delta$ is called ‘Reflection Procedure’. The procedure is very similar to the quantum rewinding technique of Watrous [Wat09], which has been used before to achieve perfect completeness for quantum multi-prover interactive proofs [KKMV08]. Also note that the idea behind the quantum rewinding technique dates back to the strong gap amplification for QMA [MW05].

It should be mentioned here that Lemma 2.16 will only be used in the honest case, while in the dishonest case we will argue about the rejection probability directly. This is why we can have a much simpler lemma compared to the description of the Reflection Procedure in [KLG13].

2.1 Choi-Jamiołkowski Representations and Post-Selection

Let $\Phi: L(\mathbb{C}^2) \rightarrow L(\mathbb{C}^2)$ be a quantum super-operator (a completely positive and trace preserving linear map). The normalized Choi-Jamiołkowski representation of Φ is defined as⁵

$$\rho_\Phi \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x,y \in \{0,1\}} \Phi(|x\rangle\langle y|) \otimes |x\rangle\langle y|, \quad \rho_\Phi \in \mathcal{D}(\mathbb{C}^4).$$

Suppose we have an EPR pair $(|\Phi^+\rangle)$ in registers (S, S') . Then ρ_Φ can be generated by applying Φ on register S . If Φ is unitary, i.e., $\Phi(\sigma) = \mathbf{U}^* \sigma \mathbf{U}$, for some unitary operator \mathbf{U} , then ρ_Φ is pure, in which case we use the notation $|J(\mathbf{U})\rangle$, where $|J(\mathbf{U})\rangle\langle J(\mathbf{U})| = \rho_\Phi$. Let $q \in [0, 1]$. By simple calculation, we get that

$$\begin{aligned} |J(\mathbf{W}_q)\rangle &= (\mathbf{W}_q \otimes \mathbb{1}) |\Phi^+\rangle = \sqrt{1-q} |\Phi^+\rangle - \iota\sqrt{q} |\Psi^+\rangle, \\ |J(\mathbf{W}_q^*)\rangle &= (\mathbf{W}_q^* \otimes \mathbb{1}) |\Phi^+\rangle = \sqrt{1-q} |\Phi^+\rangle + \iota\sqrt{q} |\Psi^+\rangle. \end{aligned}$$

⁵The Choi-Jamiołkowski representation is obviously defined for any dimension, but in this paper we will only need it for qubits, so we will be fine with this restricted definition.

In Algorithm 2, on page 13, we will be given two copies of $|J(\mathbf{W}_q^*)\rangle$ and we will have to create the state $\mathbf{W}_q|0\rangle$ with the help of the first copy. Using the second copy, we will need to apply \mathbf{W}_q^* on an arbitrary input state. The way these can be done is as follows. Suppose now that we are given $|J(\mathbf{W}_q^*)\rangle$ and we want to create $\mathbf{W}_q|0\rangle$. This can easily be done by applying the following unitary

$$\mathbf{T} \stackrel{\text{def}}{=} |00\rangle\langle\Phi^+| - |10\rangle\langle\Psi^+| + |01\rangle\langle\Phi^-| - |11\rangle\langle\Psi^-|, \quad (7)$$

because $\mathbf{T}|J(\mathbf{W}_q^*)\rangle = (\mathbf{W}_q|0\rangle) \otimes |0\rangle$. Now assume that we want to apply \mathbf{W}_q^* on an arbitrary state $|\varphi\rangle$, with the help of $|J(\mathbf{W}_q^*)\rangle$. This can be accomplished with probability $1/2$ by a procedure that we call post-selection. The procedure is described in Algorithm 1. Note that Algorithm 1 is basically teleportation, where we want to teleport the state of X (let's say it's $|\varphi\rangle$) to register S . If we get output $|\Phi^+\rangle$ then no correction is needed in the teleportation. Since \mathbf{W}_q^* was applied to S before, we get $\mathbf{W}_q^*|\varphi\rangle$ in S . If the output is $|\Psi^+\rangle$ then there is a 'Pauli- X error' in the teleportation so we get $\mathbf{W}_q^*X|\varphi\rangle$, which we can correct since \mathbf{W}_q^* and X commute. In case of the other two outputs ($|\Phi^-\rangle$ and $|\Psi^-\rangle$), there is a Z or a Y error that we can't correct, so we declare failure. This idea of simulating a quantum operator with Choi-Jamiołkowski representations has appeared before in the context of quantum interactive proof and quantum Merlin-Arthur proof systems, such as in Refs. [BSW11, KLG13]. We state a lemma here that we will use in the honest case. In the dishonest case, we will argue about the success probability and the output of Algorithm 1 in the analysis of Algorithm 2.

Lemma 2.17. *Suppose that the inputs to Algorithm 1 are $|J(\mathbf{W}_q^*)\rangle$ in (S, S') , for some $q \in [0, 1]$, and an arbitrary $|\varphi\rangle$ in X . Then the algorithm will succeed with probability $1/2$ and in that case it will output $\mathbf{W}_q^*|\varphi\rangle$ in S .*

2.2 Quantum Merlin-Arthur Proof Systems

Before we define the complexity class QMA, let us briefly describe what we mean by polynomial-time quantum algorithms or quantum verifiers. Quantum verifiers are polynomial-time uniformly generated quantum circuits consisting of some universal set of gates. There are many different universal sets and we assume that one of them has been chosen beforehand. Usually it doesn't matter which set we choose when we define quantum verifiers and classes like BQP or QMA, because it is known that each universal set can approximate any other set with exponential precision. However, in the paper we will have quantum proof systems with one-sided error, in which case the gate set may matter. This is because simulating one set of gates with another may

Algorithm 1 Post-Selection

INPUT: single qubit registers S, S', X $\{(S, S') \text{ are supposed to contain the state } |J(\mathbf{W}_q^*)\rangle.\}$

OUTPUT: success and S , or failure

- 1: Perform a measurement in the Bell basis on (S', X) .
 - 2: **IF** the output is $|\Phi^+\rangle$ **THEN**
 - 3: **RETURN** success and S
 - 4: **ELSE IF** the output is $|\Psi^+\rangle$ **THEN**
 - 5: Apply X on S .
 - 6: **RETURN** success and S
 - 7: **ELSE**
 - 8: **RETURN** failure
 - 9: **END IF**
-

ruin the one-sided error property. In this paper, we only assume that the verifier can perform or perfectly simulate the **CNOT** and the **H** gate with his universal set, besides being able to perform any polynomial-time classical computation. Note that with **CNOT** and **H**, one can perform all Pauli operators, as well as operator **T**, defined by Eq. (7). The above assumption is enough for our result, so we won't bother about the gate set in the rest of the paper.

Definition 2.18 ([Wat00, AN02]). For functions $c, s: \mathbb{Z}^+ \rightarrow (0, 1]$, a language L is in $\text{QMA}(c, s)$ if there exists a quantum verifier V with the following properties. For all $n \in \mathbb{Z}^+$ and inputs $x \in \{0, 1\}^n$, the circuit of V on input x , denoted by \mathbf{V}_x , is a polynomial-time uniformly generated quantum circuit acting on two polynomial-size registers \mathcal{P} and \mathcal{A} . One output qubit of \mathbf{V}_x is designated as the acceptance qubit. We say that \mathbf{V}_x on input $|\varphi\rangle_{\mathcal{P}} \otimes |\bar{0}\rangle_{\mathcal{A}}$ accepts if the acceptance qubit of $\mathbf{V}_x (|\varphi\rangle_{\mathcal{P}} \otimes |\bar{0}\rangle_{\mathcal{A}})$ is projected to $|1\rangle$ and we say that \mathbf{V}_x rejects if it's projected to $|0\rangle$. \mathbf{V}_x must satisfy the following properties.

Completeness. If $x \in L$ then there exists a quantum state $|\varphi\rangle \in \mathcal{P}$ such that the acceptance probability of \mathbf{V}_x , on input $|\varphi\rangle \otimes |\bar{0}\rangle_{\mathcal{A}}$, is at least $c(n)$.

Soundness. If $x \notin L$ then for all states $|\varphi\rangle \in \mathcal{P}$, \mathbf{V}_x accepts with probability at most $s(n)$, given $|\varphi\rangle \otimes |\bar{0}\rangle_{\mathcal{A}}$ as its input.

Note that \mathcal{P} is the register in which the verifier receives his proof and \mathcal{A} is his private register, which is, without loss of generality, always initialized to $|\bar{0}\rangle$. Without causing confusion, we will denote both the circuit of the verifier and the unitary operator it represents by \mathbf{V}_x .

Definition 2.19. The class QMA is defined as $\text{QMA} \stackrel{\text{def}}{=} \text{QMA}\left(\frac{2}{3}, \frac{1}{3}\right)$.

The choice of the constants in the above definition are arbitrary, as shown by the following theorem.

Theorem 2.20 ([KSV02, AN02, MW05]). *Let $c \in (0, 1)$ be a constant and $p(n)$ be a positive polynomial in n . It holds that*

$$\text{QMA} = \text{QMA}\left(c, c - \frac{1}{p(n)}\right) = \text{QMA}\left(1 - 2^{-p(n)}, 2^{-p(n)}\right).$$

Definition 2.21. The class $\text{QMA}^{\text{const-EPR}}(c, s)$ is defined the same way as $\text{QMA}(c, s)$ in Definition 2.18, except that before the prover sends the proof to the verifier, they can share a constant number of EPR pairs (the two-qubit state $|\Phi^+\rangle$).

Definition 2.22. The class $\text{QMA}_1^{\text{const-EPR}}$ is defined as $\text{QMA}_1^{\text{const-EPR}} \stackrel{\text{def}}{=} \text{QMA}^{\text{const-EPR}}(1, 1/2)$.

Similarly as before, the choice of $1/2$ is arbitrary. This is because a $\text{QMA}_1^{\text{const-EPR}}$ proof system is a special case of a two-message QIP_1 proof system and perfect parallel repetition holds even for three-message QIP_1 [KW00]. So we have the following lemma.

Lemma 2.23. *Let $p(n)$ be a positive polynomial in n . It holds that*

$$\text{QMA}_1^{\text{const-EPR}} = \text{QMA}^{\text{const-EPR}}\left(1, 1 - \frac{1}{p(n)}\right) = \text{QMA}^{\text{const-EPR}}\left(1, 2^{-p(n)}\right).$$

3 Proof of Theorem 1.1

Before we give the detailed proof of Theorem 1.1, let us briefly describe the intuition behind our proof. We also point out the similarities and the differences between our proof and the proof in [KLG13].

3.1 The Idea Behind the Proof

The basic idea to achieve perfect completeness is very similar to Ref. [KLG13]. For any input x , let us define

$$\mathbf{M}_x \stackrel{\text{def}}{=} (\mathbb{1}_{\mathcal{P}} \otimes |\bar{0}\rangle\langle\bar{0}|_{\mathcal{A}}) \mathbf{V}_x^* \Pi_{\text{acc}} \mathbf{V}_x (\mathbb{1}_{\mathcal{P}} \otimes |\bar{0}\rangle\langle\bar{0}|_{\mathcal{A}}),$$

where \mathbf{V}_x is the same as in Section 2.2 and Π_{acc} is the projector that corresponds to projecting the acceptance qubit of \mathbf{V}_x to $|1\rangle$. Note that $0 \leq \mathbf{M}_x \leq \mathbb{1}_{\mathcal{P} \otimes \mathcal{A}}$. As was observed in [MW05], the maximum acceptance probability of \mathbf{V}_x is $\|\mathbf{M}_x\|_{\infty}$, or in other words, the maximum eigenvalue of \mathbf{M}_x . We will use Lemma 2.16 to construct a test that succeeds with probability 1 in case $x \in L$. In order to achieve this, we need that for all $x \in L$, $\|\mathbf{M}_x\|_{\infty} = 1/2$. Unfortunately, this is not true in general. Instead, we have that if $x \in L$ then $\|\mathbf{M}_x\|_{\infty} \geq 1/2$. Our first objective is to modify \mathbf{M}_x such that its maximum eigenvalue is exactly $1/2$. We do this by using an auxiliary qubit (stored in register \mathcal{S}) and defining

$$\begin{aligned} \mathbf{M}'_x &\stackrel{\text{def}}{=} \mathbf{M}_x \otimes (|0\rangle\langle 0|_{\mathcal{S}} \mathbf{W}_q^* |1\rangle\langle 1|_{\mathcal{S}} \mathbf{W}_q |0\rangle\langle 0|_{\mathcal{S}}) \\ &= (\mathbb{1}_{\mathcal{P}} \otimes |\bar{0}\rangle\langle\bar{0}|_{\mathcal{A} \otimes \mathcal{S}}) (\mathbf{V}_x \otimes \mathbf{W}_q)^* (\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{\mathcal{S}}) (\mathbf{V}_x \otimes \mathbf{W}_q) (\mathbb{1}_{\mathcal{P}} \otimes |\bar{0}\rangle\langle\bar{0}|_{\mathcal{A} \otimes \mathcal{S}}), \end{aligned}$$

where $q \stackrel{\text{def}}{=} \frac{1}{2p} \in [\frac{1}{2}, 1]$. It is now easy to see that $\|\mathbf{M}'_x\|_{\infty} = 1/2$ and we can also write \mathbf{M}'_x as $\mathbf{M}'_x = \Delta \Pi \Delta$, for

$$\Delta \stackrel{\text{def}}{=} \mathbb{1}_{\mathcal{P}} \otimes |\bar{0}\rangle\langle\bar{0}|_{\mathcal{A} \otimes \mathcal{S}} \quad \text{and} \quad \Pi \stackrel{\text{def}}{=} (\mathbf{V}_x \otimes \mathbf{W}_q)^* (\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{\mathcal{S}}) (\mathbf{V}_x \otimes \mathbf{W}_q).$$

Now, we can use Lemma 2.16 and obtain the following test. Let the principal eigenvector of \mathbf{M}'_x (that corresponds to eigenvalue $1/2$) be denoted by $|\omega\rangle_{\mathcal{P}} \otimes |\bar{0}\rangle_{\mathcal{A} \otimes \mathcal{S}}$. The test receives this eigenstate as the input, applies the unitary operator $\mathbb{1} - 2\Pi$, and performs a measurement defined by operators $\{\Delta, \mathbb{1} - \Delta\}$. If the state is projected to Δ the test rejects and otherwise it accepts. Lemma 2.16 guarantees that we never project to Δ .

However, a polynomial-time verifier may not be able to perform this test, because it is possible that \mathbf{W}_q can't be expressed by a polynomial-size quantum circuit and the verifier may not even know the exact value of q . To overcome this difficulty, the verifier expects the prover to give several copies of the normalized Choi-Jamiołkowski representations of \mathbf{W}_q^* , besides $|\omega\rangle_{\mathcal{P}}$. As explained in Section 2.1, these can be used to perform \mathbf{W}_q and \mathbf{W}_q^* , by using unitary \mathbf{T} to do \mathbf{W}_q , and Algorithm 1 to do \mathbf{W}_q^* . Note that Algorithm 1 may fail, in which case we have to accept in order to maintain perfect completeness. This is the main idea to prove perfect completeness, and it is basically the same as in [KLG13].

The harder part is to prove the soundness and this is where our proof differs from the one in [KLG13]. Let us first give a high-level overview of the soundness proof of Kobayashi et al. [KLG13]. The main idea in their proof is to perform a sequence of tests (i.e., quantum algorithms with measurements at the end), which together ensure that the registers that are supposed to contain the Choi-Jamiołkowski representations of the desired operator, actually contain the Choi-Jamiołkowski representations of *some* operator. Then they show that doing the so-called ‘Reflection Simulation Test’, the one just described above, with these states in the registers, will cause rejection with some constant probability. The tests they use to ensure that the states are close to Choi-Jamiołkowski representations are the ‘Distillation Procedure’ (which is used to remove the entanglement between the register of the original proof and the registers of the Choi-Jamiołkowski representations), the ‘Space Restriction Test’ (which tests that the states are in a certain subspace), and the SWAP Test. In their analysis they also use the de Finetti theorem. We don't describe these tests here, as the interested reader can find them in [KLG13]. We just list them in order to compare them to the tools we use.

Our main idea behind the soundness proof is conceptually different. We don't argue that the states are close to Choi-Jamiołkowski representations, but we analyze our version of the Reflection Simulation Test directly. As we described this test above, there are two measurements in it. The first measurement is in Algorithm 1 and the second is given by $\{\Delta, \mathbb{1} - \Delta\}$. So, roughly speaking, we have to prove two things. First, we have to show that Algorithm 1 can't always fail, as otherwise we would end up always accepting without reaching the end of the procedure. This will be formalized later in Lemma 3.3. In order to prove Lemma 3.3, we only need two assumptions. The first assumption is that the state being measured in Algorithm 1 is separable, which is guaranteed by the de Finetti theorem (Theorem 2.14). The second assumption is that the state of some registers is close to being completely mixed, which is obviously true because these registers hold parts of EPR pairs.

The second part of the soundness proof is to show that conditioned on Algorithm 1 being successful, we get a state that projects to Δ with constant probability. To prove this, we first argue that the private register of the verifier (register A) projects to $|\bar{0}\rangle\langle\bar{0}|$. This follows from simple properties of the trace distance. We then show that the state of register S projects to $|0\rangle\langle 0|$. To prove this, we use the SWAP Test on the registers that are supposed to contain the Choi-Jamiołkowski representations. This ensures that the state of these registers are close to the same pure state. This property is formalized in Lemma 3.4. We also use a simplified version of the Space Restriction Test, which is not really a test but an application of a super-operator on the above mentioned registers. This super-operator will be defined later in Eq. (8). We can think of it as performing a projective measurement that corresponds to the Space Restriction Test and forgetting the outcome. Using the above tools, it will follow by direct calculation that the state of S projects to $|0\rangle\langle 0|$.

Note that we don't use the Distillation Procedure of [KLG13] and we use a simpler form of the Space Restriction Test. Besides that, it's worth mentioning that the tools we use can be grouped into two sets based on whether we use them in the analysis of the first or the second measurement. For the analysis of the first measurement, we need that some state is close to being maximally mixed, while in the analysis of the second, we use the SWAP Test and the above mentioned super-operator. One exception is the de Finetti theorem, as we need that the states are separable in both parts. This property of the proof may be useful for simplifying it further, because for example, to omit the SWAP Test, one would only need to re-prove that the state of S projects to $|0\rangle\langle 0|$ in the last measurement.

3.2 The Detailed Proof

This section presents the detailed proof of Theorem 1.1. Let $L \in \text{QMA}$ and V be the corresponding verifier. Let x be an input to language L and let us denote its length by n . We denote the circuit of V on input x (and also the unitary transformation it represents) by \mathbf{V}_x . Let the private register of \mathbf{V}_x be denoted by A and the register in which the proof is received by P. As in the previous section, let $\Pi_{\text{acc}} \in L(\mathcal{P} \otimes \mathcal{A})$ be the projector that corresponds to projecting the acceptance qubit of \mathbf{V}_x to $|1\rangle$. By Theorem 2.20, we assume that the completeness of V is at least $1/2$ and his soundness is at most 4^{-n} . Let $N \stackrel{\text{def}}{=} 2^{107}$. We construct a verifier W which recognizes the same language L with completeness 1, constant soundness, and with the additional property that W possesses N halves of EPR pairs in registers S'_1, \dots, S'_N before the protocol begins. The other halves of the EPR pairs are held by the prover. W gets his proof in registers P, S_1, \dots, S_N , where the S_i 's are single qubit registers, which had contained the other halves of the EPR pairs before the prover performed some transformation on them. W expects to get the original proof of V in P and the state of each (S_i, S'_i) is supposed to be $|J(\mathbf{W}_q^*)\rangle$, for some $q \in [0, 1]$. In the description of W we will use the following notations. Let \mathcal{W}^+ be the subspace of \mathbb{C}^4 spanned

by $|\Phi^+\rangle$ and $|\Psi^+\rangle$, and \mathcal{W}^- be the subspace spanned by $|\Phi^-\rangle$ and $|\Psi^-\rangle$. Let

$$\Pi^+ \stackrel{\text{def}}{=} |\Phi^+\rangle\langle\Phi^+| + |\Psi^+\rangle\langle\Psi^+| \quad \text{and} \quad \Pi^- \stackrel{\text{def}}{=} |\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-|,$$

i.e., the projections to subspaces \mathcal{W}^+ and \mathcal{W}^- . Let $\Psi : L(\mathbb{C}^4) \rightarrow L(\mathbb{C}^4)$ be a quantum super-operator defined as

$$\Psi(\mathbf{A}) \stackrel{\text{def}}{=} \Pi^+ \mathbf{A} \Pi^+ + \Pi^- \mathbf{A} \Pi^-. \quad (8)$$

\mathbf{T} still denotes the operator defined by Eq. (7). With these notations, the procedure of W is described in Algorithm 2.

Note that Algorithm 2 runs in polynomial time and besides performing the circuit \mathbf{V}_x and its inverse, it only uses \mathbf{H} , \mathbf{CNOT} , \mathbf{T} , Pauli gates, and classical logical gates. (This justifies our assumption we made about the gate set in Section 2.2.) We have to prove completeness and soundness in order to prove Theorem 1.1. Lemma 3.1 proves that in the honest case W always accepts, while Lemma 3.2 proves that in the dishonest case W rejects with probability at least 2^{-52} . This shows that $L \in \text{QMA}^{\text{const-EPR}}(1, 1 - 2^{-52})$. By Lemma 2.23, $\text{QMA}^{\text{const-EPR}}(1, 1 - 2^{-52}) = \text{QMA}_1^{\text{const-EPR}}$ so Theorem 1.1 follows.

Lemma 3.1 (Completeness). *If $x \in L$ then the prover can prepare registers P, S_1, \dots, S_N in such a way that verifier W of Algorithm 2 accepts with probability 1.*

Proof. Let $p_x \in [1/2, 1]$ be the maximum probability with which V can be made to accept x , where the maximum is taken over all states in P . Let

$$q \stackrel{\text{def}}{=} \frac{1}{2p}$$

and note that $q \in [1/2, 1]$. The honest Merlin prepares $|\omega_x\rangle$ in P , where $|\omega_x\rangle$ is the original witness of V that makes it accept with probability exactly p_x . Furthermore, for all $i \in \{1, 2, \dots, N\}$, Merlin applies \mathbf{W}_q^* to S_i . This creates $|J(\mathbf{W}_q^*)\rangle$ in all (S_i, S_i') . Then Merlin sends registers P, S_1, \dots, S_N to W .

Note that steps 1 and 2 of Algorithm 2 don't change the state because

$$|J(\mathbf{W}_q^*)\rangle = \sqrt{1-q}|\Phi^+\rangle + \iota\sqrt{q}|\Psi^+\rangle \in \mathcal{W}^+.$$

If, in step 3, b is chosen to be 1 then the SWAP Test in step 21 succeeds with certainty, by Theorem 2.15. So, from now on, suppose that b is chosen to be 0, in which case we continue to step 5. From the arguments of Section 2.1, we have that the state of S_1 after step 5 is $\mathbf{W}_q|0\rangle$. So the state of (P, A, S_1) before entering step 10 is

$$(\mathbf{V}_x^* \otimes \mathbb{1}_{S_1}) (\mathbb{1} - 2\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{S_1}) (\mathbf{V}_x \otimes \mathbf{W}_q) (|\omega_x\rangle_P \otimes |\bar{0}\rangle_A \otimes |0\rangle_{S_1}).$$

We assume that Algorithm 1 in step 10 succeeds, as otherwise we accept. In this case, by Lemma 2.17, the state of (P, A, S_2) after step 10 will be

$$(\mathbf{V}_x^* \otimes \mathbf{W}_q^*) (\mathbb{1} - 2\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{S_2}) (\mathbf{V}_x \otimes \mathbf{W}_q) (|\omega_x\rangle_P \otimes |\bar{0}\rangle_A \otimes |0\rangle_{S_2}).$$

Let

$$\Delta \stackrel{\text{def}}{=} \mathbb{1}_P \otimes |\bar{0}\rangle\langle\bar{0}|_A \otimes |0\rangle\langle 0|_{S_2} \quad \text{and} \quad \Pi \stackrel{\text{def}}{=} (\mathbf{V}_x^* \Pi_{\text{acc}} \mathbf{V}_x) \otimes (\mathbf{W}_q^* |1\rangle\langle 1|_{S_2} \mathbf{W}_q).$$

Algorithm 2 Description of verifier W in the proof of Theorem 1.1.

INPUT: description of a circuit \mathbf{V}_x , polynomial-size register P compatible with \mathbf{V}_x , and single qubit registers $S_1, \dots, S_N, S'_1, \dots, S'_N$, where the state of (S'_1, \dots, S'_N) is guaranteed to be $\mathbb{1}/2^N$. *{For all i , (S_i, S'_i) are supposed to contain $|J(\mathbf{W}_q^*)\rangle$.}*

OUTPUT: accept or reject

- 1: Permute registers $(S_1, S'_1), \dots, (S_N, S'_N)$ uniformly at random and discard all but (S_1, S'_1) and (S_2, S'_2) .
- 2: Apply Ψ on both (S_1, S'_1) and (S_2, S'_2) .
- 3: Choose $b \in_{\mathbb{R}} \{0, 1\}$ uniformly at random.
- 4: **IF** $b = 0$ **THEN**
- 5: Apply \mathbf{T} on (S_1, S'_1) . *{This creates $\mathbf{W}_q|0\rangle$ in S_1 . S'_1 can be discarded.}*
- 6: Create register A , compatible with \mathbf{V}_x , and initialize its state to $|\bar{0}\rangle$.
- 7: Apply \mathbf{V}_x on (P, A) .
- 8: Apply a phase-flip if both the acceptance qubit and register S_1 are 1. *{This is done by applying the unitary $\mathbb{1}_{P \otimes A \otimes S_1} - 2\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{S_1}$ on (P, A, S_1) .}*
- 9: Apply \mathbf{V}_x^* on (P, A) .
- 10: Execute Algorithm 1 with input (S_2, S'_2, S_1) .
- 11: **IF** Algorithm 1 fails **THEN**
- 12: **RETURN** accept
- 13: **END IF**
- 14: Measure (A, S_2) in the standard basis.
- 15: **IF** the output of the measurement is $\bar{0}$ **THEN**
- 16: **RETURN** reject
- 17: **ELSE**
- 18: **RETURN** accept
- 19: **END IF**
- 20: **ELSE**
- 21: Apply the SWAP Test on (S_1, S'_1) and (S_2, S'_2) .
- 22: **IF** the SWAP Test succeeds **THEN**
- 23: **RETURN** accept
- 24: **ELSE**
- 25: **RETURN** reject
- 26: **END IF**
- 27: **END IF**

Note that the maximum eigenvalue of operator $\Delta\Pi\Delta$ is $1/2$, with corresponding eigenstate $|\omega_x\rangle_P \otimes |\bar{0}\rangle_{A \otimes S_2}$. From Lemma 2.16,

$$\begin{aligned} 0 &= \Delta(\mathbb{1} - 2\Pi)\Delta\left(|\omega_x\rangle_P \otimes |\bar{0}\rangle_{A \otimes S_2}\right) \\ &= \left(\mathbb{1}_P \otimes |\bar{0}\rangle\langle\bar{0}|_{A \otimes S_2}\right) \left(\mathbf{V}_x^* \otimes \mathbf{W}_q^*\right) \left(\mathbb{1} - 2\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{S_2}\right) \left(\mathbf{V}_x \otimes \mathbf{W}_q\right) \left(|\omega_x\rangle_P \otimes |\bar{0}\rangle_{A \otimes S_2}\right). \end{aligned}$$

It means that the measurement of step 14 will never output $\bar{0}$. This finishes the proof of the lemma. \square

Lemma 3.2 (Soundness). *Let $x \notin L$ and n sufficiently large. Suppose that the input to Algorithm 2 is such that the reduced state on (S'_1, \dots, S'_N) is $\mathbb{1}/2^N$. Then Algorithm 2 rejects with probability at least 2^{-52} .*

Proof. Let's denote the state of $(P, S_1, S'_1, S_2, S'_2)$, after step 1, by ρ_1 . Theorem 2.14 implies that

$$d\left(\text{Tr}_{\mathcal{P}}(\rho_1), \sum_{i=1}^m p_i \xi_i \otimes \xi_i\right) \leq \frac{16}{N}.$$

Let's denote the state of the same registers, after step 2, by ρ_2 . It can be checked by direct calculation that

$$\text{Tr}_{\mathcal{P} \otimes \mathcal{S}_1 \otimes \mathcal{S}_2}(\rho_2) = \frac{\mathbb{1}_{\mathcal{S}'_1 \otimes \mathcal{S}'_2}}{4}. \quad (9)$$

From Theorem 2.7, it holds that

$$d\left(\text{Tr}_{\mathcal{P}}(\rho_2), \sum_{i=1}^m p_i \sigma_i \otimes \sigma_i\right) \leq \frac{16}{N},$$

where $\sigma_i \stackrel{\text{def}}{=} \Psi(\xi_i)$. By Lemma 2.12, there exists a ρ'_2 such that

$$\text{Tr}_{\mathcal{P}}(\rho'_2) = \sum_{i=1}^m p_i \sigma_i \otimes \sigma_i$$

and

$$d(\rho_2, \rho'_2) \leq \sqrt{\frac{32}{N}}. \quad (10)$$

Let us suppose, from now on, that before entering step 3 the state of the system is ρ'_2 . This will result in a bias of at most $\sqrt{32/N}$ in the trace distance in the rest of the states that we calculate. Throughout the rest of the proof, we will assume that the SWAP Test on input $\text{Tr}_{\mathcal{P}}(\rho'_2)$ rejects with probability at most $\varepsilon \stackrel{\text{def}}{=} 2 \cdot 2^{-52} + \sqrt{32/N} = 2^{-50}$, as otherwise we are done with the proof. With this in mind, the rest of the proof will only deal with the case when b is chosen to be 0 in step 3. In this case we continue to step 5. With these assumptions, the state of the system after step 5 is

$$\rho_5 \stackrel{\text{def}}{=} \left(\mathbf{T} \otimes \mathbb{1}_{\mathcal{P} \otimes \mathcal{S}_2 \otimes \mathcal{S}'_2}\right) \rho'_2 \left(\mathbf{T}^* \otimes \mathbb{1}_{\mathcal{P} \otimes \mathcal{S}_2 \otimes \mathcal{S}'_2}\right).$$

Let's denote the state of the whole system after step 7 by

$$\rho_7 \stackrel{\text{def}}{=} \left(\mathbf{V}_x \otimes \mathbb{1}_{\mathcal{S}_1 \otimes \mathcal{S}'_1 \otimes \mathcal{S}_2 \otimes \mathcal{S}'_2}\right) (|\bar{0}\rangle\langle\bar{0}|_{\mathcal{A}} \otimes \rho_5) \left(\mathbf{V}_x^* \otimes \mathbb{1}_{\mathcal{S}_1 \otimes \mathcal{S}'_1 \otimes \mathcal{S}_2 \otimes \mathcal{S}'_2}\right).$$

Since the acceptance probability of \mathbf{V}_x is at most 4^{-n} , we have that

$$\text{Tr}(\rho_7 \tilde{\Pi}_{\text{acc}}) \leq \frac{1}{4^n},$$

where $\tilde{\Pi}_{\text{acc}} \stackrel{\text{def}}{=} \Pi_{\text{acc}} \otimes \mathbb{1}_{\mathcal{S}_1 \otimes \mathcal{S}'_1 \otimes \mathcal{S}_2 \otimes \mathcal{S}'_2}$. Let ρ'_7 be the projection of ρ_7 to the rejection subspace, i.e.,

$$\rho'_7 \stackrel{\text{def}}{=} \frac{\left(\mathbb{1} - \tilde{\Pi}_{\text{acc}}\right) \rho_7 \left(\mathbb{1} - \tilde{\Pi}_{\text{acc}}\right)}{\text{Tr}\left(\rho_7 \left(\mathbb{1} - \tilde{\Pi}_{\text{acc}}\right)\right)}.$$

From Lemma 2.10 and Theorem 2.11, we have that

$$1 - \frac{1}{4^n} \leq \text{F}(\rho_7, \rho'_7)^2 \leq 1 - d(\rho_7, \rho'_7)^2$$

from which it follows that

$$d(\rho_7, \rho'_7) \leq \frac{1}{2^n}.$$

Now suppose that before entering step 8 the state of the system is ρ'_7 instead of ρ_7 . This will result in an additional bias of at most 2^{-n} in the trace distance in the rest of the states that we calculate. Since ρ'_7 lies in the rejection subspace,

$$\left((\mathbb{1} - 2\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{S_1}) \otimes \mathbb{1}_{S'_1 \otimes S_2 \otimes S'_2} \right) \rho'_7 \left((\mathbb{1} - 2\Pi_{\text{acc}} \otimes |1\rangle\langle 1|_{S_1}) \otimes \mathbb{1}_{S'_1 \otimes S_2 \otimes S'_2} \right) = \rho'_7,$$

which means that step 8 doesn't change the state. So the state of the system before entering step 9 is ρ'_7 . Let us change the state again, at this time from ρ'_7 back to ρ_7 . This will result in another bias of at most 2^{-n} . If the state of the system is ρ_7 before entering step 9 then the state after step 9 will be

$$\left(\mathbf{V}_x^* \otimes \mathbb{1}_{S_1 \otimes S'_1 \otimes S_2 \otimes S'_2} \right) \rho_7 \left(\mathbf{V}_x \otimes \mathbb{1}_{S_1 \otimes S'_1 \otimes S_2 \otimes S'_2} \right) = |\bar{0}\rangle\langle \bar{0}|_{\mathcal{A}} \otimes \rho_5.$$

From Lemma 3.4, together with the assumption we made about the success probability of the SWAP Test, we get that there exists a set of states $\{|\varphi_i\rangle : |\varphi_i\rangle \in \mathcal{W}^+ \text{ or } |\varphi_i\rangle \in \mathcal{W}^-\}$ such that

$$d\left(\text{Tr}_{\mathcal{P}}(\rho'_2), \sum_{i=1}^m p_i (|\varphi_i\rangle\langle \varphi_i|)^{\otimes 2} \right) \leq 6\sqrt{\varepsilon}. \quad (11)$$

This implies that

$$d(\text{Tr}_{\mathcal{P}}(\rho_5), \rho_9) \leq 6\sqrt{\varepsilon},$$

where

$$\rho_9 \stackrel{\text{def}}{=} \sum_{i=1}^m p_i (\mathbf{T}|\varphi_i\rangle\langle \varphi_i|\mathbf{T}^*) \otimes |\varphi_i\rangle\langle \varphi_i|, \quad \rho_9 \in \mathcal{D}(S_1 \otimes S'_1 \otimes S_2 \otimes S'_2).$$

Now let us change the state of (S_1, S'_1, S_2, S'_2) from $\text{Tr}_{\mathcal{P}}(\rho_5)$ to ρ_9 . This will result in another bias of at most $6\sqrt{\varepsilon}$. (Note that \mathcal{P} is not touched by the algorithm after step 9, so we don't keep track of its state.) From Eqs. (9), (10), and (11), it follows that

$$d\left(\text{Tr}_{S_1 \otimes S_2} \left(\sum_{i=1}^m p_i (|\varphi_i\rangle\langle \varphi_i|)^{\otimes 2} \right), \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4} \right) \leq \sqrt{\frac{32}{N}} + 6\sqrt{\varepsilon} < \frac{1}{8}.$$

So ρ_9 satisfies the requirements of Lemma 3.3 below. This means that Algorithm 1 in step 10 succeeds with probability at least 2^{-20} , in which case we continue to step 14.

We now argue that, conditioned on Algorithm 1 being successful, the measurement in step 14 outputs $\bar{0}$ with certainty. This will finish the proof. Note that Algorithm 1 can't change the state of \mathcal{A} as it was independent of (S_2, S'_2, S_1) before executing Algorithm 1. So before entering step 14, the state of \mathcal{A} is still $|\bar{0}\rangle$. Now we argue that after successfully executing Algorithm 1, the state of S_2 will be $|0\rangle$. Let us take some $|\varphi\rangle \in S_1 \otimes S'_1$ that belongs to either \mathcal{W}^+ or \mathcal{W}^- . Here we only argue about the case when $|\varphi\rangle \in \mathcal{W}^+$ as the other case can be proven by exactly the same way. We can write $|\varphi\rangle$ as

$$|\varphi\rangle = a|\Phi^+\rangle + b|\Psi^+\rangle, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

It is easy to see that after applying \mathbf{T} to $|\varphi\rangle$, the resulting state on S_1 will be $a|0\rangle - b|1\rangle$. Suppose that the state of (S_2, S'_2) is $|\varphi\rangle$ and the state of S_1 is $a|0\rangle - b|1\rangle$. It can be shown by direct calculation that

$$\left(|1\rangle\langle 1|_{S_2} \otimes |\Phi^+\rangle\langle \Phi^+|_{S'_2 \otimes S_1} \right) |\varphi\rangle \otimes (a|0\rangle - b|1\rangle) = 0.$$

This means that if Algorithm 1 is executed with the above input and the measurement in the algorithm results in $|\Phi^+\rangle$, then the state of S_2 will be $|0\rangle$. Similarly to the above, it can also be shown that

$$\left(|0\rangle\langle 0|_{S_2} \otimes |\Psi^+\rangle\langle \Psi^+|_{S'_2 \otimes S_1}\right) |\varphi\rangle \otimes (a|0\rangle - b|1\rangle) = 0.$$

This means that if the measurement in Algorithm 1 results in $|\Psi^+\rangle$ then the state of S_2 will be $|1\rangle$. In this case, Algorithm 1 applies \mathbf{X} on S_2 so the state of this register, after the algorithm, will be $|0\rangle$. Since ρ_9 is a convex combination of states of the above form, we got that if the state of (S_1, S'_1, S_2, S'_2) is ρ_9 , before entering step 10, then Algorithm 1 succeeds with probability at least 2^{-20} and, conditioned on success, Algorithm 2 rejects in step 16 with certainty.

However, we did modify the state during our analysis four times, so we have to account for the bias they caused, which is at most

$$\frac{1}{2^{n-1}} + \sqrt{\frac{32}{N}} + 6\sqrt{\varepsilon}.$$

So the real rejection probability, with the original input, is at least

$$\frac{1}{2^{20}} - \left(\frac{1}{2^{n-1}} + \sqrt{\frac{32}{N}} + 6\sqrt{\varepsilon}\right) = \frac{1}{2^{21}} - \frac{1}{2^{n-1}} \geq \frac{1}{2^{22}},$$

where the last inequality is true for $n \geq 23$. \square

Lemma 3.3. *Suppose that before entering step 10 of Algorithm 2, the state of (S_1, S'_1, S_2, S'_2) is*

$$\rho \stackrel{\text{def}}{=} \sum_{i=1}^m p_i (\mathbf{T}\sigma_i\mathbf{T}^*) \otimes \sigma_i,$$

for some $m \in \mathbb{Z}^+$, probability distribution $\{p_i : i = 1, \dots, m\}$, and states $\sigma_i \in \mathcal{D}(S_2 \otimes S'_2) \cong \mathcal{D}(S_1 \otimes S'_1)$. Further assume that

$$d\left(\text{Tr}_{S_1 \otimes S_2} \left(\sum_{i=1}^m p_i \sigma_i \otimes \sigma_i\right), \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4}\right) \leq \frac{1}{8}. \quad (12)$$

Then Algorithm 1, in step 10, will succeed with probability at least 2^{-20} .

The idea behind the proof of Lemma 3.3 is very simple. We show that if the measurement in Algorithm 1 fails with high probability on a state of the form $\text{Tr}_{S_2}(\sigma_i) \otimes \zeta$, where $\zeta \in \mathcal{D}(S_1)$ is an arbitrary state, then $\text{Tr}_{S_2}(\sigma_i)$ must be close to either $|\phi^+\rangle$ or $|\phi^-\rangle$. But then the convex combination of the states $\text{Tr}_{S_1}(\sigma_i) \otimes \text{Tr}_{S_2}(\sigma_i)$ won't be close to the maximally mixed state.

Proof of Lemma 3.3. Let us group the states in ensemble ρ with respect to their reduced state on S'_2 being close to $|\phi^+\rangle$, or to $|\phi^-\rangle$, or being far from both. Formally, let $\varepsilon_1 \stackrel{\text{def}}{=} 2^{-9}$,

$$\begin{aligned} A^+ &\stackrel{\text{def}}{=} \{i : 1 \leq i \leq m, d(\text{Tr}_{S_2}(\sigma_i), |\phi^+\rangle\langle \phi^+|) \leq \varepsilon_1\}, \\ A^- &\stackrel{\text{def}}{=} \{i : 1 \leq i \leq m, d(\text{Tr}_{S_2}(\sigma_i), |\phi^-\rangle\langle \phi^-|) \leq \varepsilon_1\}, \\ B &\stackrel{\text{def}}{=} \{1, 2, \dots, m\} \setminus (A^+ \cup A^-). \end{aligned}$$

Since $d(|\phi^+\rangle, |\phi^-\rangle) = 1$ and $\varepsilon_1 < 1/2$, from the triangle inequality we have that $A^+ \cap A^- = \emptyset$.

We first show that if the probability of B is at least $\varepsilon_2 \stackrel{\text{def}}{=} 1/4$ then we are done. So assume for now that $\varepsilon_2 \leq \sum_{i \in B} p_i$. For all $i \in B$ we have that

$$\sqrt{\langle \phi^+ | \text{Tr}_{S_2}(\sigma_i) | \phi^+ \rangle} = F(\text{Tr}_{S_2}(\sigma_i), |\phi^+\rangle\langle\phi^+|) \quad (13)$$

$$\leq \sqrt{1 - d(\text{Tr}_{S_2}(\sigma_i), |\phi^+\rangle\langle\phi^+|)^2} \quad (14)$$

$$< \sqrt{1 - \varepsilon_1^2}, \quad (15)$$

where (13) follows from (2), (14) follows from Theorem 2.11, and (15) is from the definition of B . The above implies that

$$\langle \phi^+ | \text{Tr}_{S_2}(\sigma_i) | \phi^+ \rangle < 1 - \varepsilon_1^2 \quad \text{and similarly} \quad \langle \phi^- | \text{Tr}_{S_2}(\sigma_i) | \phi^- \rangle < 1 - \varepsilon_1^2.$$

From the above and using the fact that

$$\langle \phi^+ | \text{Tr}_{S_2}(\sigma_i) | \phi^+ \rangle + \langle \phi^- | \text{Tr}_{S_2}(\sigma_i) | \phi^- \rangle = \text{Tr}(\text{Tr}_{S_2}(\sigma_i)) = 1,$$

we get that

$$\varepsilon_1^2 < \langle \phi^+ | \text{Tr}_{S_2}(\sigma_i) | \phi^+ \rangle \quad \text{and} \quad \varepsilon_1^2 < \langle \phi^- | \text{Tr}_{S_2}(\sigma_i) | \phi^- \rangle.$$

Let us take an arbitrary state

$$|\psi\rangle \stackrel{\text{def}}{=} a|\phi^+\rangle + b|\phi^-\rangle \in \mathcal{S}_1, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

If the state of (S'_2, S_1) , in the input to Algorithm 1, is $\text{Tr}_{S_2}(\sigma_i) \otimes |\psi\rangle\langle\psi|$ then the algorithm will succeed with probability

$$\begin{aligned} \text{Tr}((\text{Tr}_{S_2}(\sigma_i) \otimes |\psi\rangle\langle\psi|) \Pi^+) &= |a|^2 \cdot \langle \phi^+ | \text{Tr}_{S_2}(\sigma_i) | \phi^+ \rangle + |b|^2 \cdot \langle \phi^- | \text{Tr}_{S_2}(\sigma_i) | \phi^- \rangle \\ &> \varepsilon_1^2 (|a|^2 + |b|^2) \\ &= \varepsilon_1^2, \end{aligned}$$

where the first equality follows from direct calculation using

$$|\Phi^+\rangle = \frac{|\phi^+\rangle \otimes |\phi^+\rangle + |\phi^-\rangle \otimes |\phi^-\rangle}{\sqrt{2}} \quad \text{and} \quad |\Psi^+\rangle = \frac{|\phi^+\rangle \otimes |\phi^+\rangle - |\phi^-\rangle \otimes |\phi^-\rangle}{\sqrt{2}}.$$

This implies that if the state of (S'_2, S_1) is $\text{Tr}_{S_2}(\sigma_i) \otimes \zeta$, for any $\zeta \in \mathcal{D}(\mathcal{S}_1)$, then the probability that Algorithm 1 succeeds is at least ε_1^2 . We got that if $\varepsilon_2 \leq \sum_{i \in B} p_i$ then Algorithm 1 succeeds with probability at least $\varepsilon_1^2 \varepsilon_2 = 2^{-20}$, in which case we are done.

So, from now on, assume that $\sum_{i \in B} p_i < \varepsilon_2$. We will show that this assumption leads to a contradiction, which will finish the proof. Lemma 2.12 implies that

$$\forall i \in A^+, \exists \tau_i \in \mathcal{D}(\mathcal{S}_2) : d(\sigma_i, \tau_i \otimes |\phi^+\rangle\langle\phi^+|) \leq \sqrt{2\varepsilon_1},$$

$$\forall i \in A^-, \exists \tau_i \in \mathcal{D}(\mathcal{S}_2) : d(\sigma_i, \tau_i \otimes |\phi^-\rangle\langle\phi^-|) \leq \sqrt{2\varepsilon_1}.$$

We now replace σ_i with $\tau_i \otimes |\phi^+\rangle\langle\phi^+|$ or $\tau_i \otimes |\phi^-\rangle\langle\phi^-|$ in ρ . Formally, let us define

$$\begin{aligned} \mu_B &\stackrel{\text{def}}{=} \sum_{i \in B} p_i (\mathbf{T} \sigma_i \mathbf{T}^*) \otimes \sigma_i, \\ \rho' &\stackrel{\text{def}}{=} \sum_{i \in A^+} p_i (\mathbf{T} (\tau_i \otimes |\phi^+\rangle\langle\phi^+|) \mathbf{T}^*) \otimes \tau_i \otimes |\phi^+\rangle\langle\phi^+| \\ &\quad + \sum_{i \in A^-} p_i (\mathbf{T} (\tau_i \otimes |\phi^-\rangle\langle\phi^-|) \mathbf{T}^*) \otimes \tau_i \otimes |\phi^-\rangle\langle\phi^-| \\ &\quad + \mu_B, \end{aligned}$$

where $\text{Tr}(\mu_B) < \varepsilon_2$. Note that $d(\rho, \rho') < 2\sqrt{2\varepsilon_1}$, which, together with (12), implies that

$$d\left(\xi, \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4}\right) \leq 2\sqrt{2\varepsilon_1} + \frac{1}{8} = \frac{1}{4}, \quad (16)$$

where

$$\xi \stackrel{\text{def}}{=} \text{Tr}_{S_1 \otimes S_2} \left(\left(\mathbf{T}^* \otimes \mathbb{1}_{S_2 \otimes S'_2} \right) \rho' \left(\mathbf{T} \otimes \mathbb{1}_{S_2 \otimes S'_2} \right) \right).$$

On the other hand, we have that

$$\xi = p_+ (|\phi^+\rangle\langle\phi^+|)^{\otimes 2} + p_- (|\phi^-\rangle\langle\phi^-|)^{\otimes 2} + \nu_B,$$

for some ν_B , where we used the shorthand $p_+ \stackrel{\text{def}}{=} \sum_{i \in A^+} p_i$ and $p_- \stackrel{\text{def}}{=} \sum_{i \in A^-} p_i$. Note that $\text{Tr}(\nu_B) < \varepsilon_2$, so Lemma 2.8 implies that

$$d\left(\xi, p_+ (|\phi^+\rangle\langle\phi^+|)^{\otimes 2} + p_- (|\phi^-\rangle\langle\phi^-|)^{\otimes 2}\right) \leq \frac{\varepsilon_2}{2}. \quad (17)$$

The following calculation will lead us to a contradiction.

$$\begin{aligned} \frac{1}{2} &\leq \frac{1}{2} \left(\left| \frac{1}{4} - p_+ \right| + \left| \frac{1}{4} - p_- \right| + \frac{1}{2} \right) \\ &= \frac{1}{2} \left\| \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4} - \left(p_+ (|\phi^+\rangle\langle\phi^+|)^{\otimes 2} + p_- (|\phi^-\rangle\langle\phi^-|)^{\otimes 2} \right) \right\|_{\text{Tr}} \end{aligned} \quad (18)$$

$$\begin{aligned} &= d\left(\frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4}, p_+ (|\phi^+\rangle\langle\phi^+|)^{\otimes 2} + p_- (|\phi^-\rangle\langle\phi^-|)^{\otimes 2}\right) \\ &\leq d\left(\xi, \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4}\right) + d\left(\xi, p_+ (|\phi^+\rangle\langle\phi^+|)^{\otimes 2} + p_- (|\phi^-\rangle\langle\phi^-|)^{\otimes 2}\right) \end{aligned} \quad (19)$$

$$\leq d\left(\xi, \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4}\right) + \frac{\varepsilon_2}{2}, \quad (20)$$

where (18) is because the eigenvalues of $\frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4} - \left(p_+ (|\phi^+\rangle\langle\phi^+|)^{\otimes 2} + p_- (|\phi^-\rangle\langle\phi^-|)^{\otimes 2} \right)$ are $\frac{1}{4} - p_+$, $\frac{1}{4} - p_-$, and $\frac{1}{4}$ with multiplicity 2. Eq. (19) follows from the triangle inequality and at (20) we used (17). Eq. (20) implies that

$$d\left(\xi, \frac{\mathbb{1}_{S'_1 \otimes S'_2}}{4}\right) \geq \frac{1}{2} - \frac{\varepsilon_2}{2} = \frac{3}{8},$$

which contradicts to (16). So we conclude that it must be that $\varepsilon_2 \leq \sum_{i \in B} p_i$, in which case Algorithm 1 succeeds with the desired probability, as argued above. \square

The following lemma is similar to Proposition 24 of [KLG13].

Lemma 3.4. *Let S_1, S'_1, S_2, S'_2 be single-qubit registers and let the state of (S_1, S'_1, S_2, S'_2) be*

$$\rho \stackrel{\text{def}}{=} \sum_{i=1}^m p_i \sigma_i \otimes \sigma_i,$$

where $m \in \mathbb{Z}^+$, $\{p_i : i = 1, \dots, m\}$ is a probability distribution, and $\sigma_i = \Psi(\xi_i)$, for some $\xi_i \in \mathcal{D}(S_1 \otimes S'_1) \cong \mathcal{D}(S_2 \otimes S'_2)$. Let $0 \leq \varepsilon < 1$. If the SWAP Test, applied between (S_1, S'_1) and (S_2, S'_2) , succeeds with probability at least $1 - \varepsilon$ then there exist a set of states

$$\{|\varphi_i\rangle : 1 \leq i \leq m, |\varphi_i\rangle \in \mathcal{W}^+ \text{ or } |\varphi_i\rangle \in \mathcal{W}^-\}$$

such that

$$d\left(\rho, \sum_{i=1}^m p_i |\varphi_i\rangle\langle\varphi_i| \otimes |\varphi_i\rangle\langle\varphi_i|\right) \leq 6\sqrt{\varepsilon}.$$

Proof. On input $\sigma_i \otimes \sigma_i$ the SWAP Test succeeds with probability $(1 + \text{Tr}(\sigma_i^2))/2$, by Theorem 2.15. So with input ρ the SWAP Test succeeds with probability

$$\sum_{i=1}^m p_i \frac{1 + \text{Tr}(\sigma_i^2)}{2} \geq 1 - \varepsilon.$$

If $\varepsilon = 0$ it implies that all σ_i 's are pure and the statement of the lemma follows. So, from now on, assume that $0 < \varepsilon$. Then the above inequality intuitively means that for most of the i 's, $\text{Tr}(\sigma_i^2)$ must be close to 1. Formally, let

$$B \stackrel{\text{def}}{=} \{i : 1 \leq i \leq m, \text{Tr}(\sigma_i^2) \leq 1 - 2\sqrt{\varepsilon}\},$$

$$A \stackrel{\text{def}}{=} \{1, 2, \dots, m\} \setminus B.$$

Suppose towards contradiction that $2\sqrt{\varepsilon} \leq \sum_{i \in B} p_i$. Then the probability that the SWAP Test fails is

$$\begin{aligned} \sum_{i=1}^m p_i \frac{1 - \text{Tr}(\sigma_i^2)}{2} &\geq \sum_{i \in B} p_i \frac{1 - \text{Tr}(\sigma_i^2)}{2} \\ &\geq \sum_{i \in B} p_i \frac{1 - (1 - 2\sqrt{\varepsilon})}{2} \\ &\geq \sqrt{\varepsilon} \cdot \sum_{i \in B} p_i \\ &\geq 2\varepsilon, \end{aligned}$$

which is a contradiction. This implies that $\sum_{i \in B} p_i < 2\sqrt{\varepsilon}$. For all $i \in A$, let λ_i be the maximum eigenvalue of σ_i and $|\varphi_i\rangle$ be the corresponding eigenstate. Note that either $|\varphi_i\rangle \in \mathcal{W}^+$ or $|\varphi_i\rangle \in \mathcal{W}^-$. From the definition of A , we have that

$$1 - 2\sqrt{\varepsilon} < \text{Tr}(\sigma_i^2) \leq \|\sigma_i\|_{\text{Tr}} \cdot \|\sigma_i\|_{\infty} = \|\sigma_i\|_{\infty} = \lambda_i,$$

where the second inequality follows from Lemma 2.2. The above calculation, together with Lemma 2.9, imply that

$$\forall i \in A : d(\sigma_i, |\varphi_i\rangle\langle\varphi_i|) \leq 2\sqrt{\varepsilon}. \quad (21)$$

We can now bound the required trace distance.

$$\begin{aligned} d\left(\rho, \sum_{i=1}^m p_i (|\varphi_i\rangle\langle\varphi_i|)^{\otimes 2}\right) &\leq d\left(\sum_{i=1}^m p_i \sigma_i^{\otimes 2}, \sum_{i \in A} p_i \sigma_i^{\otimes 2}\right) + d\left(\sum_{i \in A} p_i \sigma_i^{\otimes 2}, \sum_{i \in A} p_i (|\varphi_i\rangle\langle\varphi_i|)^{\otimes 2}\right) \\ &\quad + d\left(\sum_{i \in A} p_i (|\varphi_i\rangle\langle\varphi_i|)^{\otimes 2}, \sum_{i=1}^m p_i (|\varphi_i\rangle\langle\varphi_i|)^{\otimes 2}\right) \end{aligned} \quad (22)$$

$$\leq 6\sqrt{\varepsilon}, \quad (23)$$

where (22) follows from the triangle inequality and at (23) we used Lemma 2.8 twice and (21). \square

Acknowledgements

The author would like to thank Rahul Jain, Sarvagya Upadhyay, and Penghui Yao for helpful discussions on the topic.

References

- [Aar09] Scott Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 9(1):81–89, January 2009, [ARXIV:0806.0450](#).
- [AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.
- [ABD⁺09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009, [ARXIV:0804.0802](#).
- [AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey. October 2002, [ARXIV:QUANT-PH/0210077](#).
- [Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the 17th annual ACM Symposium on Theory of Computing*, STOC '85, pages 421–429, 1985.
- [BBD⁺97] Adriano Barenco, André Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, 1997, [ARXIV:QUANT-PH/9604028](#).
- [BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, September 2001, [ARXIV:QUANT-PH/0102001](#).
- [Boo12] Adam D. Bookatz. QMA-complete problems. December 2012, [ARXIV:1212.6312](#).
- [Bra06] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. February 2006, [ARXIV:QUANT-PH/0602108](#).
- [BSW11] Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7(1):101–117, 2011, [ARXIV:1004.0411](#).
- [BT09] Hugue Blier and Alain Tapp. All languages in NP have very short quantum proofs. In *Third International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, 2009, [ARXIV:0709.0738](#).
- [CKMR07] Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007, [ARXIV:QUANT-PH/0602130](#).
- [GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

- [GN13] David Gosset and Daniel Nagaj. Quantum 3-SAT is QMA_1 -complete. February 2013, [ARXIV:1302.0290](#).
- [GS86] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th annual ACM Symposium on Theory of Computing*, STOC '86, pages 59–68, 1986.
- [HM10] Aram W. Harrow and Ashley Montanaro. An efficient test for product states with applications to quantum Merlin-Arthur games. In *51st Annual IEEE Symposium on Foundations of Computer Science*, pages 633–642, 2010, [ARXIV:1001.0017](#).
- [JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. In *Proceedings of the 42nd annual ACM Symposium on Theory of Computing*, STOC '10, pages 573–582, 2010, [ARXIV:0907.4737](#).
- [JKNN12] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):461–471, May 2012, [ARXIV:1111.5306](#).
- [JN12] Rahul Jain and Ashwin Nayak. Short proofs of the quantum substate theorem. *IEEE Transactions on Information Theory*, 58(6):3664–3669, June 2012, [ARXIV:1103.6067](#).
- [KKMV08] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. In *23rd Annual IEEE Conference on Computational Complexity*, pages 211–222, June 2008, [ARXIV:0711.3715](#).
- [KKR06] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006, [ARXIV:QUANT-PH/0406180](#).
- [KLG13] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, ITCS '13, pages 329–352, New York, NY, USA, 2013. ACM, [ARXIV:1210.1290](#).
- [KMY03] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Algorithms and Computation*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198. Springer Berlin / Heidelberg, 2003, [ARXIV:QUANT-PH/0306051](#).
- [Kni96] Emanuel Knill. Quantum randomness and nondeterminism. October 1996, [ARXIV:QUANT-PH/9610012](#).
- [KSV02] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalıy. *Classical and Quantum Computation*. American Mathematical Society, 2002.
- [KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd annual ACM Symposium on Theory of Computing*, STOC '00, pages 608–617, 2000.

- [LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, October 1992.
- [MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005, [ARXIV:CS/0506068](#).
- [NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [NWZ09] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information and Computation*, 9(11):1053–1068, November 2009, [ARXIV:0904.1549](#).
- [Per12] Attila Pereszlényi. Multi-prover quantum Merlin-Arthur proof systems with small gap. May 2012, [ARXIV:1205.2761](#).
- [Sha92] Adi Shamir. $IP = PSPACE$. *Journal of the ACM*, 39(4):869–877, October 1992.
- [She92] A. Shen. $IP = PSPACE$: Simplified proof. *Journal of the ACM*, 39(4):878–880, October 1992.
- [Vya03] Mikhail N. Vyalyi. QMA = PP implies that PP contains PH. Technical Report 21 (2003), Electronic Colloquium on Computational Complexity, April 2003. [TR03-021](#).
- [Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual IEEE Symposium on Foundations of Computer Science*, pages 537–546, 2000, [ARXIV:CS/0009002](#).
- [Wat03] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.
- [Wat08a] John Watrous. Quantum computational complexity. April 2008, [ARXIV:0804.3401](#).
- [Wat08b] John Watrous. Theory of quantum information. Lecture notes from Fall 2008, <https://cs.uwaterloo.ca/~watrous/quant-info/>, 2008.
- [Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009, [ARXIV:QUANT-PH/0511020](#).
- [Win99] Andreas Winter. *Coding Theorems of Quantum Information Theory*. PhD thesis, Universität Bielefeld, 1999, [ARXIV:QUANT-PH/9907077](#).
- [ZF87] Stathis Zachos and Martin Fürer. Probabilistic quantifiers vs. distrustful adversaries. In *Proceedings of the Seventh Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 287 of *Lecture Notes in Computer Science*, pages 443–455, London, UK, 1987. Springer-Verlag.