Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?*

Hirotada Kobayashi[a b †]
hirotada@nii.ac.jp

Keiji Matsumoto[a b ‡]
keiji@nii.ac.jp

Tomoyuki Yamakami[c §]
yamakami@u-fukui.ac.jp

[a]Principles of Informatics Research Division
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

[b]Quantum Computation and Information Project
Solution Oriented Research for Science and Technology
Japan Science and Technology Agency
5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

[c]Department of Information Science
Graduate School of Engineering
University of Fukui
3-9-1 Bunkyo, Fukui City, Fukui 910-8507, Japan

Abstract

This paper introduces quantum "multiple-Merlin"-Arthur proof systems in which Arthur receives multiple quantum proofs that are unentangled with each other. Although classical multi-proof systems are obviously equivalent to classical single-proof systems (i.e., standard Merlin-Arthur proof systems), it is unclear whether or not quantum multi-proof systems collapse to quantum single-proof systems (i.e., standard quantum Merlin-Arthur proof systems). This paper presents a way of reducing the number of proofs to two while keeping the two-sided bounded-error property, which gives a necessary and sufficient condition under which the number of quantum proofs is reducible to two. It is also proved that, in the case of perfect soundness, using multiple quantum proofs does not increase the power of quantum Merlin-Arthur proof systems.

[*] A preliminary version of this paper has appeared in *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198, 2003 [35].

[†] Work partly done while at Department of Information Science, Graduate School of Science, The University of Tokyo and Quantum Computation and Information Project, Exploratory Research for Advanced Technology, Japan Science and Technology Agency. Partially supported by the Grant-in-Aid for Scientific Research (B) Nos. 18300002 and 21300002 of the Ministry of Education, Culture, Sports, Science and Technology of Japan.

[‡] Work partly done while at Quantum Computation and Information Project, Exploratory Research for Advanced Technology, Japan Science and Technology Agency. Partially supported by the Grant-in-Aid for Scientific Research (B) Nos. 18300002 and 21300002 of the Ministry of Education, Culture, Sports, Science and Technology of Japan.

[§] Work partly done while at School of Information Technology and Engineering, University of Ottawa and School of Computer Science and Engineering, University of Aizu.

1 Introduction

1.1 Background

Merlin-Arthur proof systems, or Merlin-Arthur games as originally called, were introduced by Babai [9]. In a Merlin-Arthur proof system, a prover (Merlin) presents a proof and a verifier (Arthur) probabilistically verifies its correctness with high success probability. The class of problems having Merlin-Arthur proof systems is denoted by MA, and has played important roles in computational complexity theory [9, 13, 11, 12, 10, 47, 44, 8, 23, 19, 18, 25, 45].

A quantum analogue of MA was first discussed by Knill [33] and has been studied intensively [31, 48, 29, 26, 49, 7, 39, 28, 1, 36, 38, 3, 5, 37]. In the most commonly-used version of quantum Merlin-Arthur proof systems, a proof presented by Merlin is a pure quantum state called a *quantum proof* and Arthur's verification process is a polynomial-time quantum computation. The corresponding complexity class is called QMA (the name QMA was first used by Watrous [48]). However, all the previous studies have considered only the model in which Arthur receives a single quantum proof, and no discussions have been done on the model in which Arthur receives *multiple* quantum proofs unentangled with each other.

Classically, multiple proofs can be concatenated into a single long proof, and thus, there is no advantage to use multiple proofs. Quantumly, however, using multiple quantum proofs may be potentially more powerful than using a single quantum proof, as it might be advantageous to Arthur to know that a given proof is a tensor product of some quantum states. One may argue that Arthur could rule out any quantum proof far from states of tensor product form in the first place, by performing some preprocessing. It turns out that this most straightforward attempt of simulating multiple quantum proofs by a single quantum proof does not work well even in the simplest case of two quantum proofs versus one — there is no physical method that determines whether a given unknown state is in a tensor product form or maximally entangled, as will be shown in Section 6. Moreover, many existing techniques that are useful when proving properties of QMA do not seem to be applicable to the multi-proof case. For example, the unpublished proof by Kitaev and Watrous that proves the containment $\mathrm{QMA} \subseteq \mathrm{PP}$ does not seem to work for the multi-proof cases. The same is true for the simplified proof by Marriott and Watrous [39] for the same statement and even for the proof of $\mathrm{QMA} \subseteq \mathrm{PSPACE}$ [31, 32]. The existing proofs for the property that parallel repetition of a single-proof system reduces the error probability to be arbitrarily small [30, 48, 32, 39] cannot be applied to the multi-proof cases, either. The multi-proof model are also important in quantum information theory, because the model is inherently related to entanglement theory. Indeed, after the completion of this work, Aaronson, Beigi, Drucker, Fefferman, and Shor [2] succeeded in proving a strong connection between our model and the famous "Additivity Conjecture" in entanglement theory, which is one of the most important conjectures in quantum information theory. Of course, it is possible that using multiple quantum proofs does not make quantum Merlin-Arthur proof systems more powerful in the complexity theoretical sense. Even in that case, using multiple proofs could make it easier to construct protocols of quantum Merlin-Arthur proof systems. Hence, the authors believe that it is important to investigate the multi-proof model of quantum Merlin-Arthur proof systems. It is interesting to note that here the *nonexistence* of entanglement among proofs may have the possibility of enhancing the verification power, unlike the usual situations of quantum information processing where we make use of the *existence* of entanglement.

1.2 Contribution of This Paper

Motivated by the observations described in the previous subsection, this paper extends the standard single-proof model of quantum Merlin-Arthur proof systems to the multi-proof model by allowing Arthur to use multiple quantum proofs, which are given in a tensor product form of multiple quantum states. One may think of this model as a special case of quantum multi-prover interactive proof systems [34] in which a verifier cannot ask questions to provers, and provers do not share entanglement a priori. Formally, we say that a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ has a (k, c, s)*-quantum Merlin-Arthur proof system* if there exists a polynomial-time quantum verifier V such that, for every input x, (i) if $x \in A_{\mathrm{yes}}$, there exists a set of $k(|x|)$ quantum proofs that makes V accept x with probability at least $c(|x|)$, and (ii) if $x \in A_{\mathrm{no}}$, for any set of $k(|x|)$ quantum proofs given, V accepts x with probability at most $s(|x|)$. The resulting complexity class is denoted by $\mathrm{QMA}(k, c, s)$. We often abbreviate $\mathrm{QMA}\big(k, \frac{2}{3}, \frac{1}{3}\big)$ as $\mathrm{QMA}(k)$ throughout this paper.[1]

Besides our central question whether or not quantum multi-proof Merlin-Arthur proof systems collapse to quantum single-proof systems, it is also unclear if there are k_1 and k_2 with $k_1 \neq k_2$ such that $\mathrm{QMA}(k_1) = \mathrm{QMA}(k_2)$. Towards settling these questions, this paper shows how the number of quantum proofs can be reduced to two while keeping the completeness-soundness gap bounded by an inverse-polynomial. More formally, let poly be the set of all polynomially bounded functions, and let poly^{-1} be the set of all inverse-polynomial functions, i.e., the set of all functions f with range $[0, 1]$ such that $f \geq \frac{1}{p}$ for some $p \in \mathrm{poly}$. The pair of functions c, s with range $(0, 1)$ is said a *two-sided bounded-error completeness-soundness pair* if $c - s \in \mathrm{poly}^{-1}$ and $2^{-p} \leq s < c \leq 1 - 2^{-p}$ for some $p \in \mathrm{poly}$. The following is the main theorem of this paper:

Theorem (Theorem 4)**.** *For any function $k \in \mathrm{poly}$ and any two-sided bounded-error completeness-soundness pair (c, s), there exists a function $p \in \mathrm{poly}$ such that, for any function $q \in \mathrm{poly}$,*

$$\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}\Big(2, 1 - 2^{-q}, 1 - \frac{1}{p}\Big).$$

The key ingredient to show this is the claim that, for any quantum multi-proof Merlin-Arthur proof system with some appropriate condition on completeness and soundness, we can reduce the number of proofs by (almost) two-thirds (where the gap between completeness and soundness becomes worse, but is still bounded by an inverse-polynomial). This is done by using the controlled-swap test, which often plays a key role in quantum computation (e.g., in Refs. [30, 17]). The idea behind this comes from the fact that two unentangled quantum states can pass the controlled-swap test with certainty if and only if they are the identical *pure* states, which may be used to detect unallowed entanglement among quantum proofs.

An important consequence of this main theorem is a necessary and sufficient condition under which the number of quantum proofs is reducible to two, which is related to the possibility of amplifying success probability of quantum two-proof Merlin-Arthur proof systems without increasing the number of quantum proofs. More formally, consider the following condition:

($*$) For any two-sided bounded-error completeness-soundness pair (c, s), $\mathrm{QMA}(2, c, s) = \mathrm{QMA}\big(2, \frac{2}{3}, \frac{1}{3}\big)$.

Then the main theorem essentially shows the following:

Corollary (Corollary 5)**.** $\mathrm{QMA}(k, c, s) = \mathrm{QMA}\big(2, \frac{2}{3}, \frac{1}{3}\big)$ *for any function $k \geq 2$ in* poly *and any two-sided bounded-error completeness-soundness pair (c, s) if and only if the condition ($*$) is satisfied*[2].

Alternative consequence is that quantum multi-proof Merlin-Arthur proof systems are equivalent to standard single-proof ones if and only if quantum *two-proof* Merlin-Arthur proof systems are equivalent to standard single-proof ones.

[1] Here we choose completeness and soundness accepting probabilities $\frac{2}{3}$ and $\frac{1}{3}$ to define the class $\mathrm{QMA}(k)$, but there may be other reasonable choices. For instance, $\mathrm{QMA}(k)$ could be defined as the union of $\mathrm{QMA}(k, 1 - \varepsilon, \varepsilon)$ for all negligible functions ε. It is possible that other reasonable definitions of $\mathrm{QMA}(k)$ form different classes from the one defined in this paper, since it is not known how to amplify the success probability of $\mathrm{QMA}(k)$. The authors believe, however, that the choice of $\frac{2}{3}$ and $\frac{1}{3}$ would best highlight the essence of the results in this paper.

[2] This improves the result proved in our preliminary conference version [35], where we required the amplifiablity of the success probability not only for two-proof systems but also for k-proof systems, for every k. Also, the statement was originally proved only for every *constant* k, whereas the improved statement in the current version holds even for every polynomially-bounded function k. The same improvements were done independently by Aaronson et al. [2].

Corollary (Corollary 6)**.** $\mathrm{QMA}(k, c, s) = \mathrm{QMA}$ *for any function* $k \in \mathrm{poly}$ *and any two-sided bounded-error completeness-soundness pair* (c, s) *if and only if* $\mathrm{QMA}(2, c, s) = \mathrm{QMA}$ *for any two-sided bounded-error completeness-soundness pair* (c, s)*.*

It is also proved that quantum multi-proof Merlin-Arthur proof systems are just as powerful as single-proof ones in the case of perfect soundness.

Theorem (Theorem 12)**.** *For any functions* $k \in \mathrm{poly}$ *and* $c \colon \mathbb{Z}^+ \to [0, 1]$*,*

$$\mathrm{QMA}(k, c, 0) = \mathrm{QMA}(1, c, 0).$$

With further analyses, the class NQP, which derives from another concept of "quantum nondeterminism" introduced by Adleman, DeMarrais, and Huang [4] and discussed by a number of studies [22, 21, 51, 50], is characterized by the union of $\mathrm{QMA}(1, c, 0)$ for all completeness probability functions c. This bridges between two existing concepts of "quantum nondeterminism".

Theorem (Theorem 15)**.** $\mathrm{NQP} = \bigcup_{c \colon \mathbb{Z}^+ \to (0,1]} \mathrm{QMA}(1, c, 0)$.

1.3 Recent Progress

After the completion of this work, a number of studies showed very intriguing properties of our model.

Liu, Christandl, and Verstraete [38] showed that the PURE STATE N-REPRESENTABILITY problem, which naturally arises in quantum chemistry, can be verified by a quantum two-proof Merlin-Arthur proof system with two-sided bounded error. Interestingly, the problem is not known to be in standard QMA.

Blier and Tapp [16] proved that the NP-complete problem GRAPH 3-COLORING has a quantum two-proof Merlin-Arthur proof system of perfect completeness with soundness bounded away from one by an inverse-polynomial, where both of the two unentangled quantum proofs consist of only logarithmically many qubits. As their system scales up, this in particular implies that, in the unbounded-error setting, the power of quantum multi-proof Merlin-Arthur proof systems equals NEXP even with only two proofs.

Aaronson et al. [2] proved that the NP-complete problem 3-SAT has a quantum multi-proof Merlin-Arthur proof system of perfect completeness with constant soundness error, where the number of proofs is almost square root of the instance size, and each quantum proof consists of only logarithmically many qubits. They further showed that the "Additivity Conjecture" would imply that any quantum two-proof Merlin-Arthur proof system can be made to have arbitrarily small two-sided bounded error, and $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ for any polynomially bounded function $k \geq 2$.

1.4 Organization of This Paper

The remainder of this paper is organized as follows. In Section 2 we give a brief review of several basic notions of quantum computation and information theory. In Section 3 we formally define the multi-proof model of quantum Merlin-Arthur proof systems. In Section 4 we show a way of reducing the number of proofs to two while keeping the two-sided bounded-error property and a condition under which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$. In Section 5 we focus on the systems of perfect soundness. In Section 6 we show that there is no physical method that determines whether a given unknown state is in a tensor product form or maximally entangled. Finally, we conclude with Section 7 which summarizes this paper. The conference version of this paper [35] also included the result that there exists an oracle relative to which $\mathrm{QMA}(k)$ does not contain co-UP. The present version omits this result, since it turned out that the statement is easily proved by using the result by Raz and Shpilka [43].

2 Preliminaries

We start with reviewing several fundamental notions used in this paper. Throughout this paper we assume that all input strings are over the alphabet $\Sigma = \{0, 1\}$, and $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively.

A function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ is *polynomially bounded* if there exists a polynomial-time deterministic Turing machine that outputs $1^{f(n)}$ on input 1^n. Let poly be the set of all polynomially bounded functions $p\colon \mathbb{Z}^+ \to \mathbb{N}$, and let poly^{-1} be the set of all functions $f\colon \mathbb{Z}^+ \to [0, 1]$ such that $f \geq \frac{1}{p}$ for some $p \in \mathrm{poly}$. The pair of functions $c, s\colon \mathbb{Z}^+ \to (0, 1)$ is said a *two-sided bounded-error completeness-soundness pair* if $c - s \in \mathrm{poly}^{-1}$ and $2^{-p} \leq s < c \leq 1 - 2^{-p}$ for some $p \in \mathrm{poly}$.

For any Hilbert space $\mathcal{H}$, let $I_{\mathcal{H}}$ denote the identity operator over $\mathcal{H}$. In this paper, all Hilbert spaces are of dimension power of two.

2.1 Quantum Fundamentals

First we briefly review basic notations and definitions in quantum computation and quantum information theory. Detailed descriptions are found in Refs. [41, 32], for instance.

A *pure quantum state*, or a *pure state* in short, is a unit vector $|\psi\rangle$ in some Hilbert space $\mathcal{H}$. For any Hilbert space $\mathcal{H}$, let $|0_{\mathcal{H}}\rangle$ denote the pure quantum state in $\mathcal{H}$ of which all the qubits are in state $|0\rangle$. A *mixed quantum state*, or a *mixed state* in short, is a classical probability distribution $(p_i, |\psi_i\rangle)$, $0 \leq p_i \leq 1$, $\sum_i p_i = 1$ over pure states $|\psi_i\rangle \in \mathcal{H}$. This can be interpreted as being in the pure state $|\psi_i\rangle$ with probability p_i. A mixed state $(p_i, |\psi_i\rangle)$ is often described in the form of a *density operator* $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Any density operator is positive semidefinite and has trace one. It should be noted that different probabilistic mixtures of pure states can yield mixed states with the identical density operator. It is also noted that there is no physical method (i.e., no measurement) to distinguish mixed states with the identical density operator. Therefore, density operators give complete descriptions of quantum states, and we may use the term “density operator” to indicate the corresponding mixed state. For any Hilbert space $\mathcal{H}$, let $\mathbf{D}(\mathcal{H})$ denote the set of density operators over $\mathcal{H}$.

One of the important operations to density operators is the *trace-out* operation. Given Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ and a quantum state with its density operator ρ in $\mathbf{D}(\mathcal{H} \otimes \mathcal{K})$, the quantum state after *tracing out* $\mathcal{K}$ has its density operator in $\mathbf{D}(\mathcal{H})$ defined by $\mathrm{tr}_{\mathcal{K}}\rho = \sum_{i=1}^{d} (I_{\mathcal{H}} \otimes \langle e_i|)\rho(I_{\mathcal{H}} \otimes |e_i\rangle)$ for any orthonormal basis $\{|e_i\rangle\}$ of $\mathcal{K}$, where d is the dimension of $\mathcal{K}$. To perform this operation on some part of a quantum system gives a partial view of the quantum system with respect to the remaining part.

A *positive operator-valued measure (POVM)* on a Hilbert space $\mathcal{H}$ is defined to be a set $\boldsymbol{M} = \{M_1, \dots, M_k\}$ of nonnegative Hermitian operators over $\mathcal{H}$ such that $\sum_{i=1}^{k} M_i = I_{\mathcal{H}}$. For any POVM $\boldsymbol{M}$ on $\mathcal{H}$, there is a quantum mechanical measurement that results in i with probability exactly $\mathrm{tr}(M_i\rho)$ for any ρ in $\mathbf{D}(\mathcal{H})$. See Refs. [24, 42] for more rigorous descriptions on quantum measurements.

The *fidelity* $F(\rho, \sigma)$ between two density operators ρ and σ in $\mathbf{D}(\mathcal{H})$ is defined by $F(\rho, \sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$. This paper uses the following two properties on fidelity.

Lemma 1 ([27]). *For any Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ and any density operators $\rho_1, \sigma_1 \in \mathbf{D}(\mathcal{H})$ and $\rho_2, \sigma_2 \in \mathbf{D}(\mathcal{K})$,*

$$F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1, \sigma_1)F(\rho_2, \sigma_2).$$

Lemma 2 ([46, 40]). *For any Hilbert space $\mathcal{H}$ and any density operators $\rho, \sigma, \xi \in \mathbf{D}(\mathcal{H})$,*

$$F(\rho, \sigma)^2 + F(\sigma, \xi)^2 \leq 1 + F(\rho, \xi).$$

2.2 Quantum Circuits

Next we review the model of quantum circuits. We use the following notion of polynomial-time uniformly generated families of quantum circuits.

A quantum circuit consists of a finite number of quantum gates that are applied in sequence to a finite number of qubits. A family $\{Q_x\}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a deterministic procedure that, on every input x, outputs a description of Q_x and runs in time polynomial in $|x|$. It is assumed that the circuits in such a family are composed of gates in some reasonable, universal, finite set of quantum gates. Furthermore, it is assumed that the number of gates in any circuit is not more than the length of the description of that circuit. Therefore Q_x must have size polynomial in $|x|$. For convenience, we may identify a circuit Q_x with the unitary operator it induces.

Since non-unitary and unitary quantum circuits are equivalent in computational power [6], it is sufficient to treat only unitary quantum circuits, which justifies the above definition. For avoiding unnecessary complication, however, the descriptions of procedures may include non-unitary operations in the subsequent sections. Even in such cases, it is always possible to construct unitary quantum circuits that essentially achieve the same procedures described.

3 Definitions

Here we formally define quantum *multi-proof* Merlin-Arthur proof systems. Although all the statements in this paper can be proved only in terms of languages without using promise problems [20], in what follows we define models and prove statements in terms of promise problems, for generality and for the compatibility with some subsequent studies on our model [38, 37].

A *quantum proof of size q* is a pure quantum state of q qubits.

A *quantum verifier V for quantum k-proof Merlin-Arthur proof systems* is a polynomial-time computable mapping of the form $V\colon \Sigma^* \to \Sigma^*$. For every input $x \in \Sigma^*$, the string $V(x)$ is interpreted as a description of a polynomial-size quantum circuit. In other words, $\{V(x)\}$ forms a polynomial-time uniformly generated family of quantum circuits. The qubits upon which each $V(x)$ acts are divided into $k+1$ sets: one set, consisting of $q_{\mathcal{V}}(|x|)$ qubits, serves as work space of V, and each of the rest k sets serves as "witness space" of V that is used for storing a quantum proof of size $q_{\mathcal{M}}(|x|)$, for some functions $q_{\mathcal{V}}, q_{\mathcal{M}} \in \mathrm{poly}$. One of the qubits in the work space of V is designated as the output qubit.

A set of k quantum proofs is *compatible* with a quantum verifier V if the size of every quantum proof coincides with the size of witness space of V.

Suppose that V receives k quantum proofs $|\phi_1\rangle, \dots, |\phi_k\rangle$. The probability that V accepts x is defined to be the probability that an observation of the output qubit in the $\{|0\rangle, |1\rangle\}$ basis yields $|1\rangle$, after the circuit $V(x)$ is applied to the state $|0_{\mathcal{V}}\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_k\rangle$, where $\mathcal{V}$ is the Hilbert space corresponding to the work space of V.

More generally, the number k of quantum proofs may not necessarily be a constant, and may be a function in poly of the input length.

Definition 3. Given functions $k \in \mathrm{poly}$ and $c, s\colon \mathbb{Z}^+ \to [0,1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{QMA}(k, c, s)$ if there exists a quantum verifier V for k-proof quantum Merlin-Arthur proof systems such that, for every x,

(Completeness) if $x \in A_{\mathrm{yes}}$, there exists a set of quantum proofs $|\phi_1\rangle, \dots, |\phi_{k(|x|)}\rangle$ compatible with V that makes V accept x with probability at least $c(|x|)$,

(Soundness) if $x \in A_{\mathrm{no}}$, for any set of quantum proofs $|\phi_1\rangle, \dots, |\phi_{k(|x|)}\rangle$ compatible with V, V accepts x with probability at most $s(|x|)$.

We say that a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ has a (k, c, s)*-quantum Merlin-Arthur proof system*, or a $\mathrm{QMA}(k, c, s)$ *proof system* in short, if and only if A is in $\mathrm{QMA}(k, c, s)$. For simplicity, we abbreviate $\mathrm{QMA}\bigl(k, \frac{2}{3}, \frac{1}{3}\bigr)$ as $\mathrm{QMA}(k)$ for every k.

Note that allowing quantum proofs of mixed states does not increase the maximal accepting probability of proof systems, which justifies the model defined above. For readability, in what follows, the arguments x and $|x|$ may be dropped in various functions, if it is not confusing.

4 Reducing the Number of Quantum Proofs

This section shows the main theorem of this paper, which states that the number of quantum proofs can be reduced to two while keeping the two-sided bounded-error property, i.e., the property that the gap between completeness and soundness is bounded by an inverse-polynomial.

Theorem 4. *For any function* $k \in \mathrm{poly}$ *and any two-sided bounded-error completeness-soundness pair* (c, s)*, there exists a function* $p \in \mathrm{poly}$ *such that, for any function* $q \in \mathrm{poly}$*,*

$$\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}\Bigl(2, 1 - 2^{-q}, 1 - \frac{1}{p}\Bigr).$$

First, assuming Theorem 4, we give a necessary and sufficient condition under which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ for any polynomially bounded function $k \geq 2$.

Consider the following condition, which essentially states that the success probability is arbitrarily amplifiable for quantum two-proof Merlin-Arthur proof systems without increasing the number of proofs:

$(*)$ For any two-sided bounded-error completeness-soundness pair (c, s), $\mathrm{QMA}(2, c, s) = \mathrm{QMA}\bigl(2, \frac{2}{3}, \frac{1}{3}\bigr)$.

This condition $(*)$ is actually necessary and sufficient for $\mathrm{QMA}(k) = \mathrm{QMA}(2)$.

Corollary 5. $\mathrm{QMA}(k, c, s) = \mathrm{QMA}\bigl(2, \frac{2}{3}, \frac{1}{3}\bigr)$ *for any function* $k \geq 2$ *in* poly *and any two-sided bounded-error completeness-soundness pair* (c, s) *if and only if the condition* $(*)$ *is satisfied.*

Proof. The "only if" part is obvious and we show the "if" part. From Theorem 4, for any function $k \in \mathrm{poly}$ and any two-sided bounded-error completeness-soundness pair (c, s), there exists a function $p \in \mathrm{poly}$ such that $\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}\bigl(2, 1 - 2^{-q}, 1 - \frac{1}{p}\bigr)$ for $q \in \mathrm{poly}$ chosen so that $\bigl(1 - 2^{-q}, 1 - \frac{1}{p}\bigr)$ is a two-sided bounded-error completeness-soundness pair. Now the condition $(*)$ ensures that $\mathrm{QMA}\bigl(2, 1 - 2^{-q}, 1 - \frac{1}{p}\bigr) = \mathrm{QMA}\bigl(2, \frac{2}{3}, \frac{1}{3}\bigr)$, and the inclusion $\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}\bigl(2, \frac{2}{3}, \frac{1}{3}\bigr)$ holds. The other inclusion is trivial, since the condition $(*)$ implies that $\mathrm{QMA}\bigl(2, \frac{2}{3}, \frac{1}{3}\bigr) = \mathrm{QMA}(2, c, s)$ for any two-sided bounded-error completeness-soundness pair (c, s). Hence the corollary follows. □

Alternatively, Theorem 4 shows a necessary and sufficient condition under which $\mathrm{QMA}(k) = \mathrm{QMA}$ for any polynomially bounded function k.

Corollary 6. $\mathrm{QMA}(k, c, s) = \mathrm{QMA}$ *for any function* $k \in \mathrm{poly}$ *and any two-sided bounded-error completeness-soundness pair* (c, s) *if and only if* $\mathrm{QMA}(2, c, s) = \mathrm{QMA}$ *for any two-sided bounded-error completeness-soundness pair* (c, s).

Proof. The proof is almost parallel to the proof of Corollary 5. Again the "only if" part is obvious and we show the "if" part. Using the same argument as in the proof of Corollary 5, for any function $k \in \mathrm{poly}$ and any two-sided bounded-error completeness-soundness pair (c, s), there exist functions $p, q \in \mathrm{poly}$ such that $\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}\bigl(2, 1 - 2^{-p}, 1 - \frac{1}{q}\bigr)$ and $\bigl(1 - 2^{-p}, 1 - \frac{1}{q}\bigr)$ is a two-sided bounded-error completeness-soundness pair. From our assumption, $\mathrm{QMA}\bigl(2, 1 - 2^{-p}, 1 - \frac{1}{q}\bigr) = \mathrm{QMA}$, and thus, the inclusion $\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}$ follows. The other inclusion is trivial since $\mathrm{QMA}(k, c, s) \supseteq \mathrm{QMA}(1, c, s) = \mathrm{QMA}$ for any two-sided bounded-error completeness-soundness pair (c, s), and the corollary follows. □

Remark. Theorem 4 and Corollary 5 improve the original statement in our conference version [35] in two ways. First, the condition $(*)$ now only requires the amplifiablity of the success probability for two-proof systems, whereas our original condition required it for every k-proof system. Second, now the statements hold even with a k-proof system for every polynomially-bounded function k. Previously, the statements were shown only for every *constant* k. The same improvements were independently done by Aaronson et al. [2] but with a different proof. Instead of repeatedly applying the transformation that reduces the number of proofs by two-thirds as above, they showed a direct method of reducing the number of proofs to two [2, Theorem 4.6]. Although the resulting two-proof system from their transformation also has soundness only polynomially bounded away from one, their soundness is better than ours in most cases (except for the case where the gap between completeness c and soundness s in the original system is so small relative to the number k of proofs that $c - s \in o(k^{-\alpha})$, where $\alpha = \frac{\log 20}{\log 3 - 1} - 1 \approx 6.388\cdots$, in which case our analysis gives better soundness).

The rest of this section is devoted to the proof of Theorem 4.

4.1 Achieving Exponentially Small Completeness Error

We first show a simple way of achieving exponentially small completeness error while keeping soundness error bounded away from one, which works well for *any* proof systems. A similar result was independently proved by Aaronson et al. [2, Lemma 2.5].

Lemma 7. *Let* $c, s \colon \mathbb{Z}^+ \to [0, 1]$ *be any functions that satisfy* $c - s \geq \frac{1}{q}$ *for some function* $q \in \mathrm{poly}$, *and let* Π *be any proof system with completeness at least* c *and soundness at most* s. *Consider another proof system* Π' *such that, for every input of length* n, Π' *carries out* $N = 2p(n)(q(n))^2$ *attempts of* Π *in parallel for a function* $p \in \mathrm{poly}$, *and accepts iff at least* $\frac{c(n)+s(n)}{2}$*-fraction of these* N *attempts results in acceptance in* Π. *Then* Π' *has completeness at least* $1 - 2^{-p}$ *and soundness at most* $\frac{2s}{c+s} \leq 1 - \frac{c-s}{2} \leq 1 - \frac{1}{2q}$.

Proof. Let X_i be the random variable that takes 1 iff the ith attempt of Π in Π' results in acceptance and otherwise takes 0, for each $1 \leq i \leq N$, and let Y be the random variable defined by $Y = \frac{\sum_{i=1}^{N} X_i}{N}$.

Noticing that the accepting probability in Π' is given by $\Pr\bigl[Y \geq \frac{c(n)+s(n)}{2}\bigr]$ and that $\mathbf{E}[Y] = \frac{\sum_{i=1}^{N} \mathbf{E}[X_i]}{N}$, the completeness bound of Π' directly follows from the Hoeffding bound while the soundness bound of Π' directly follows from Markov's inequality. □

The following is an immediate corollary of Lemma 7.

Corollary 8. *For any functions* $k, p \in \mathrm{poly}$ *and any two-sided bounded-error completeness-soundness pair* (c, s),

$$\mathrm{QMA}(k, c, s) \subseteq \mathrm{QMA}\Bigl(k, 1 - 2^{-p}, \frac{2s}{c+s}\Bigr) \subseteq \mathrm{QMA}\Bigl(k, 1 - 2^{-p}, 1 - \frac{c-s}{2}\Bigr).$$

4.2 Controlled-Swap Test with Mixed States

Next we show a fundamental property of the controlled-swap test when applied to a pair of mixed states. This property is easy to prove. To the best knowledge of the authors, however, it has not appeared previously, and the authors believe that this property will be useful in many cases.

The controlled-swap operator exchanges the contents of two registers R_1 and R_2 if the control register B contains 1, and does nothing if B contains 0. Given a pair of mixed states ρ and σ of n qubits of the form $\rho \otimes \sigma$, prepare quantum registers B, R_1, and R_2. The register B consists of only one qubit that is initially set to state $|0\rangle$, while the registers R_1 and R_2 consist of n qubits and ρ and σ are initially set in R_1 and R_2, respectively. The controlled-swap test is performed by running the algorithm described in Figure 1.

Controlled-Swap Test

1. Apply the Hadamard transformation H to B.
2. Apply the controlled-swap operator to R_1 and R_2 using B as a control qubit. That is, swap the contents of R_1 and R_2 if B contains 1, and do nothing if B contains 0.
3. Apply the Hadamard transformation H to B. Accept if B contains 0, and reject otherwise.

Figure 1: The controlled-swap test.

Proposition 9. *The probability that the input pair of mixed states ρ and σ is accepted in the controlled-swap test is exactly $\frac{1}{2} + \frac{1}{2}\mathrm{tr}(\rho\sigma)$.*

Proof. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ denote the Hilbert spaces corresponding to R_1 and R_2, respectively. Let $\rho = \sum_i p_i |e_i\rangle\langle e_i|$ and $\sigma = \sum_i q_i |f_i\rangle\langle f_i|$ be the decompositions of ρ and σ with respect to some orthonormal bases $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ of $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively. Then the state in $(\mathsf{R}_1, \mathsf{R}_2)$ is $|e_i\rangle \otimes |f_j\rangle$ with probability $p_i q_j$, and in such a case, the test results in acceptance with probability $\frac{1}{2} + \frac{|\langle e_i|f_j\rangle|^2}{2}$. Therefore, the states ρ and σ are accepted with probability

$$\begin{aligned}
\sum_i \sum_j p_i q_j \left(\frac{1}{2} + \frac{|\langle e_i|f_j\rangle|^2}{2} \right) &= \frac{1}{2} + \frac{1}{2} \sum_i \sum_j p_i q_j \langle e_i|f_j\rangle\langle f_j|e_i\rangle \\
&= \frac{1}{2} + \frac{1}{2} \sum_i \sum_j p_i q_j \mathrm{tr}(|e_i\rangle\langle e_i|f_j\rangle\langle f_j|) \\
&= \frac{1}{2} + \frac{1}{2} \mathrm{tr}\Big[\Big(\sum_i p_i |e_i\rangle\langle e_i| \Big) \Big(\sum_j q_j |f_j\rangle\langle f_j| \Big) \Big] \\
&= \frac{1}{2} + \frac{1}{2} \mathrm{tr}(\rho\sigma),
\end{aligned}$$

as desired. □

4.3 Key Lemma and Proof of Theorem 4

Using Proposition 9, we can show the following lemma, which is the key to proving Theorem 4.

Lemma 10. *For any function $k \in \mathrm{poly}$, any $r \in \{0, 1, 2\}$, and any functions $\varepsilon, \delta \colon \mathbb{Z}^+ \to [0, 1]$ satisfying $\delta > 10\varepsilon$,*

$$\mathrm{QMA}(3k + r, 1 - \varepsilon, 1 - \delta) \subseteq \mathrm{QMA}\Big(2k + r, 1 - \frac{\varepsilon}{2}, 1 - \frac{\delta}{20}\Big).$$

The essence of the proof of Lemma 10 is the basis case where $k = 1$ and $r = 0$. We first give a proof for this particular case, which will be helpful to see the idea.

Proposition 11. *For any functions $\varepsilon, \delta \colon \mathbb{Z}^+ \to [0, 1]$ satisfying $\delta > 10\varepsilon$,*

$$\mathrm{QMA}(3, 1 - \varepsilon, 1 - \delta) \subseteq \mathrm{QMA}\Big(2, 1 - \frac{\varepsilon}{2}, 1 - \frac{\delta}{20}\Big).$$

Verifier's Protocol in Two-Proof System

1. Receive the first quantum proof $|\psi_1\rangle$ in $(\mathsf{R}_1, \mathsf{S}_1)$ and the second quantum proof $|\psi_2\rangle$ in $(\mathsf{R}_2, \mathsf{S}_2)$.

2. Do one of the following two tests uniformly at random.

   2.1 (SEPARABILITY TEST)
   Perform the controlled-swap test over S_1 and S_2 using B as a control qubit. That is, perform the following:

   2.1.1 Apply the Hadamard transformation H to B.

   2.1.2 Apply the controlled-swap operator to S_1 and S_2 using B as a control qubit.

   2.1.3 Apply the Hadamard transformation H to B. Accept if B contains 0, and reject otherwise.

   2.2 (SIMULATION TEST)
   Apply $V(x)$ to the qubits in $(\mathsf{V}, \mathsf{R}_1, \mathsf{R}_2, \mathsf{S}_1)$. Accept iff the result corresponds to the accepting computation of the original quantum verifier.

Figure 2: Verifier's protocol in two-proof system.

Proof. Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem in $\mathrm{QMA}(3, 1-\varepsilon, 1-\delta)$. Given a $\mathrm{QMA}(3, 1-\varepsilon, 1-\delta)$ proof system for A, we construct a $\mathrm{QMA}\bigl(2, 1-\frac{\varepsilon}{2}, 1-\frac{\delta}{20}\bigr)$ proof system for A in the following way.

Let V be the quantum verifier of the original $\mathrm{QMA}(3, 1-\varepsilon, 1-\delta)$ proof system. For every input x, suppose that V uses $q_{\mathcal{V}}(|x|)$ private qubits, and each of the quantum proofs V receives consists of $q_{\mathcal{M}}(|x|)$ qubits, for some functions $q_{\mathcal{V}}, q_{\mathcal{M}} \in \mathrm{poly}$. Let $V(x)$ be the unitary transformation V applies. Our new quantum verifier W in the $\mathrm{QMA}\bigl(2, 1-\frac{\varepsilon}{2}, 1-\frac{\delta}{20}\bigr)$ proof system prepares quantum registers R_1, R_2, S_1, and S_2 for quantum proofs and V and B for his private computation. Each R_i and S_i consists of $q_{\mathcal{M}}(|x|)$ qubits, V consists of $q_{\mathcal{V}}(|x|)$ qubits, and B consists of a single qubit. All the qubits in (V, B) are initialized to state $|0\rangle$. W receives two quantum proofs $|\psi_1\rangle$ and $|\psi_2\rangle$ of $2q_{\mathcal{M}}(|x|)$ qubits in $(\mathsf{R}_1, \mathsf{S}_1)$ and $(\mathsf{R}_2, \mathsf{S}_2)$, respectively, which are expected to be of the form

$$|\psi_1\rangle = |\phi_1\rangle \otimes |\phi_3\rangle, \qquad |\psi_2\rangle = |\phi_2\rangle \otimes |\phi_3\rangle,$$

where each $|\phi_i\rangle$ is the ith quantum proof the original quantum verifier V would receive. Of course, each $|\psi_i\rangle$ may not be of the form above and the first and the second $q_{\mathcal{M}}(|x|)$ qubits of $|\psi_i\rangle$ may be entangled. Let $\mathcal{V}$, $\mathcal{B}$, each $\mathcal{R}_i$, and each $\mathcal{S}_i$ be the Hilbert spaces corresponding to the quantum registers V, B, R_i, and S_i, respectively. The protocol of W is described in Figure 2.

The intuitive idea behind this protocol is that, if there are little entanglement between S_i and R_i for both of $i \in \{1, 2\}$, the SIMULATION TEST succeeds in simulating the original system with high probability, while if S_i is unallowably entangled with R_i for at least one of $i \in \{1, 2\}$, the SEPARABILITY TEST results in rejection with high probability. In what follows, we formally prove that this intuition indeed is correct.

First, for the completeness, suppose that the input x is in A_{yes}. In the original proof system, there exist quantum proofs $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_3\rangle$ that cause the original quantum verifier V to accept x with probability at least $1-\varepsilon$. In the constructed protocol, let the quantum proofs $|\psi_1\rangle$ and $|\psi_2\rangle$ be of the form $|\psi_1\rangle = |\phi_1\rangle \otimes |\phi_3\rangle$ and $|\psi_2\rangle = |\phi_2\rangle \otimes |\phi_3\rangle$. Then it is obvious that the constructed quantum verifier W accepts x with certainty in the SEPARABILITY TEST and with probability at least $1-\varepsilon$ in the SIMULATION TEST, and the completeness follows.

Now for the soundness, assume that the input x is in A_{no}. Consider any pair of quantum proofs $|\psi'_1\rangle$ and $|\psi'_2\rangle$ of $2q_{\mathcal{M}}(|x|)$ qubits, which are set in the pairs of the quantum registers $(\mathsf{R}_1, \mathsf{S}_1)$ and $(\mathsf{R}_2, \mathsf{S}_2)$, respectively. Let $\rho = \mathrm{tr}_{\mathcal{R}_1} |\psi'_1\rangle\langle\psi'_1|$ and $\sigma = \mathrm{tr}_{\mathcal{R}_2} |\psi'_2\rangle\langle\psi'_2|$.

(i) In the case $\mathrm{tr}(\rho\sigma) \leq 1 - \frac{\delta}{5}$:
In this case, by Proposition 9, the probability p_{sep} that the input x is accepted in the SEPARABILITY TEST is given and bounded from above by

$$p_{\mathrm{sep}} = \frac{1}{2} + \frac{1}{2}\mathrm{tr}(\rho\sigma) \leq \frac{1}{2} + \frac{1}{2}\Bigl(1 - \frac{\delta}{5}\Bigr) = 1 - \frac{\delta}{10}.$$

Thus the verifier W accepts the input x with probability at most $\frac{1}{2} + \frac{p_{\mathrm{sep}}}{2} \leq 1 - \frac{\delta}{20}$.

(ii) In the case $\mathrm{tr}(\rho\sigma) > 1 - \frac{\delta}{5}$:
Let $\widetilde{V} = V(x) \otimes I_{\mathcal{S}_2}$ and $\widetilde{\Pi}_{\mathrm{acc}} = \Pi_{\mathrm{acc}} \otimes I_{\mathcal{S}_2}$, where Π_{acc} is the projection onto accepting states of the original proof system. For notational convenience, here it is assumed that $\widetilde{V}$ and $\widetilde{\Pi}_{\mathrm{acc}}$ are applied to $(\mathsf{V}, \mathsf{R}_1, \mathsf{S}_1, \mathsf{R}_2, \mathsf{S}_2)$ in this order of registers, although the registers to which $V(x)$ and Π_{acc} are applied are assumed to be in the order of V, R_1, R_2, and S_1.

Define two quantum states $|\alpha\rangle$ and $|\beta\rangle$ by

$$|\alpha\rangle = |0_{\mathcal{V}}\rangle \otimes |\psi'_1\rangle \otimes |\psi'_2\rangle, \qquad |\beta\rangle = \frac{1}{\bigl\|\widetilde{\Pi}_{\mathrm{acc}}\widetilde{V}|\alpha\rangle\bigr\|}\widetilde{\Pi}_{\mathrm{acc}}\widetilde{V}|\alpha\rangle.$$

Then, noticing that

$$\bigl\|\widetilde{\Pi}_{\mathrm{acc}}\widetilde{V}|\alpha\rangle\bigr\| = \frac{1}{\bigl\|\widetilde{\Pi}_{\mathrm{acc}}\widetilde{V}|\alpha\rangle\bigr\|}\bigl|\langle\alpha|\widetilde{V}^\dagger\widetilde{\Pi}_{\mathrm{acc}}\widetilde{V}|\alpha\rangle\bigr| = F\bigl(|\beta\rangle\langle\beta|, \widetilde{V}|\alpha\rangle\langle\alpha|\widetilde{V}^\dagger\bigr) = F\bigl(\widetilde{V}^\dagger|\beta\rangle\langle\beta|\widetilde{V}, |\alpha\rangle\langle\alpha|\bigr),$$

the probability p_{sim} that the input x is accepted in the SIMULATION TEST is given by

$$p_{\mathrm{sim}} = \bigl\|\widetilde{\Pi}_{\mathrm{acc}}\widetilde{V}|\alpha\rangle\bigr\|^2 = F\bigl(\widetilde{V}^\dagger|\beta\rangle\langle\beta|\widetilde{V}, |\alpha\rangle\langle\alpha|\bigr)^2.$$

The fact $\mathrm{tr}(\rho\sigma) > 1 - \frac{\delta}{5}$ implies that the maximum eigenvalue λ of ρ satisfies $\lambda > 1 - \frac{\delta}{5}$. Thus there exists a pure state $|\phi'_1\rangle \in \mathcal{R}_1 \otimes \mathcal{S}_1$ of the form $|\phi'_1\rangle = |\xi'_1\rangle \otimes |\eta'_1\rangle$ for some $|\xi'_1\rangle \in \mathcal{R}_1$ and $|\eta'_1\rangle \in \mathcal{S}_1$ such that

$$F\bigl(|\phi'_1\rangle\langle\phi'_1|, |\psi'_1\rangle\langle\psi'_1|\bigr) > \sqrt{1 - \frac{\delta}{5}},$$

by using the Schmidt decomposition and that $\rho = \mathrm{tr}_{\mathcal{R}_1}|\psi'_1\rangle\langle\psi'_1|$. Similarly, the maximum eigenvalue of σ is more than $1 - \frac{\delta}{5}$ and there exists $|\phi'_2\rangle \in \mathcal{R}_2 \otimes \mathcal{S}_2$ of the form $|\phi'_2\rangle = |\xi'_2\rangle \otimes |\eta'_2\rangle$ for some $|\xi'_2\rangle \in \mathcal{R}_2$ and $|\eta'_2\rangle \in \mathcal{S}_2$ such that

$$F\bigl(|\phi'_2\rangle\langle\phi'_2|, |\psi'_2\rangle\langle\psi'_2|\bigr) > \sqrt{1 - \frac{\delta}{5}}.$$

Therefore, letting $|\gamma\rangle = |0_{\mathcal{V}}\rangle \otimes |\phi'_1\rangle \otimes |\phi'_2\rangle$, we have from Lemma 1 that

$$F(|\alpha\rangle\langle\alpha|, |\gamma\rangle\langle\gamma|) > 1 - \frac{\delta}{5}.$$

Furthermore, together with the facts that $\Pi_{\mathrm{acc}}|\beta\rangle = |\beta\rangle$ and that $|\beta\rangle$ is a unit vector, it follows from the soundness condition of the original proof system that

$$F\bigl(\widetilde{V}^\dagger|\beta\rangle\langle\beta|\widetilde{V}, |\gamma\rangle\langle\gamma|\bigr) = |\langle\beta|\widetilde{V}|\gamma\rangle| = |\langle\beta|\Pi_{\mathrm{acc}}\widetilde{V}|\gamma\rangle| \leq \bigl\|\Pi_{\mathrm{acc}}\widetilde{V}|\gamma\rangle\bigr\| \leq \sqrt{1-\delta}.$$

Using Lemma 2, we have that

$$F\bigl(\widetilde{V}^\dagger|\beta\rangle\langle\beta|\widetilde{V}, |\alpha\rangle\langle\alpha|\bigr)^2 + F(|\alpha\rangle\langle\alpha|, |\gamma\rangle\langle\gamma|)^2 \leq 1 + F\bigl(\widetilde{V}^\dagger|\beta\rangle\langle\beta|\widetilde{V}, |\gamma\rangle\langle\gamma|\bigr).$$

It follows that

$$\begin{aligned} p_{\text{sim}} &\leq 1 + F\bigl(\widetilde{V}^{\dagger}|\beta\rangle\langle\beta|\widetilde{V}, |\gamma\rangle\langle\gamma|\bigr) - F(|\alpha\rangle\langle\alpha|, |\gamma\rangle\langle\gamma|)^2 \\ &< 1 + \sqrt{1-\delta} - \Bigl(1 - \frac{\delta}{5}\Bigr)^2 \leq 2 - \frac{\delta}{2} - 1 + \frac{2\delta}{5} - \frac{\delta^2}{25} \leq 1 - \frac{\delta}{10}. \end{aligned}$$

Thus the verifier W accepts the input x with probability at most $\frac{1}{2} + \frac{p_{\text{sim}}}{2} \leq 1 - \frac{\delta}{20}$.

Hence the soundness is at most $1 - \frac{\delta}{20}$, as required. □

Now we prove Lemma 10.

Proof of Lemma 10. The proof is a simple generalization of the case of Proposition 11.

Let $A = \{A_{\text{yes}}, A_{\text{no}}\}$ be a problem in $\text{QMA}(3k + r, 1 - \varepsilon, 1 - \delta)$. Given a $\text{QMA}(3k + r, 1 - \varepsilon, 1 - \delta)$ proof system for A, we construct a $\text{QMA}\bigl(2k + r, 1 - \frac{\varepsilon}{2}, 1 - \frac{\delta}{20}\bigr)$ proof system for A in the following way.

Let V be the quantum verifier of the original $\text{QMA}(3k + r, 1 - \varepsilon, 1 - \delta)$ proof system. For every input x, suppose that V uses $q_{\mathcal{V}}(|x|)$ private qubits, and each of quantum proofs V receives consists of $q_{\mathcal{M}}(|x|)$ qubits, for some functions $q_{\mathcal{V}}, q_{\mathcal{M}} \in \text{poly}$. Let $V(x)$ be the unitary transformation V applies. Our new quantum verifier W in the $\text{QMA}\bigl(2k + r, 1 - \frac{\varepsilon}{2}, 1 - \frac{\delta}{20}\bigr)$ proof system prepares quantum registers $\mathsf{R}_{1,1}, \ldots, \mathsf{R}_{1,k}$, $\mathsf{R}_{2,1}, \ldots, \mathsf{R}_{2,k}$, $\mathsf{S}_{1,1}, \ldots, \mathsf{S}_{1,k}$, $\mathsf{S}_{2,1}, \ldots, \mathsf{S}_{2,k}$, $\mathsf{R}_{3,1}, \ldots, \mathsf{R}_{3,r}$, $\mathsf{S}_{3,1}, \ldots, \mathsf{S}_{3,r}$ for quantum proofs and quantum registers V and B for his private computation. Each of $\mathsf{R}_{i,j}$ and $\mathsf{S}_{i,j}$ consists of $q_{\mathcal{M}}(|x|)$ qubits, V consists of $q_{\mathcal{V}}(|x|)$ qubits, and B consists of a single qubit. All the qubits in (V, B) are initialized to state $|0\rangle$. Let $\mathcal{V}$, $\mathcal{B}$, each $\mathcal{R}_{i,j}$, and each $\mathcal{S}_{i,j}$ be the Hilbert spaces corresponding to the quantum registers V, B, $\mathsf{R}_{i,j}$, and $\mathsf{S}_{i,j}$, respectively. W receives $2k + r$ quantum proofs $|\psi_{1,1}\rangle, \ldots, |\psi_{1,k}\rangle$, $|\psi_{2,1}\rangle, \ldots, |\psi_{2,k}\rangle$, and $|\psi_{3,1}\rangle, \ldots, |\psi_{3,r}\rangle$ of $2q_{\mathcal{M}}(|x|)$ qubits in $(\mathsf{R}_{1,1}, \mathsf{S}_{1,1}), \ldots, (\mathsf{R}_{1,k}, \mathsf{S}_{1,k})$, $(\mathsf{R}_{2,1}, \mathsf{S}_{2,1}), \ldots, (\mathsf{R}_{2,k}, \mathsf{S}_{2,k})$, and $(\mathsf{R}_{3,1}, \mathsf{S}_{3,1}), \ldots, (\mathsf{R}_{3,r}, \mathsf{S}_{3,r})$, respectively, which are expected to be of the form

$$\begin{aligned} |\psi_{1,j_1}\rangle &= |\phi_{j_1}\rangle \otimes |\phi_{2k+j_1}\rangle, \\ |\psi_{2,j_1}\rangle &= |\phi_{k+j_1}\rangle \otimes |\phi_{2k+j_1}\rangle, \\ |\psi_{3,j_2}\rangle &= |\phi_{3k+j_2}\rangle \otimes |0_{\mathcal{S}_{3,j_2}}\rangle, \end{aligned}$$

for each $1 \leq j_1 \leq k$ and $1 \leq j_2 \leq r$, where each $|\phi_i\rangle$ is the ith quantum proof the original quantum verifier V would receive. The protocol of W is described in Figure 3.

The rest of the proof is essentially the same as in the case of Proposition 11. When analyzing soundness, consider any set of $2k + r$ quantum proofs $|\psi'_{1,1}\rangle, \ldots, |\psi'_{1,k}\rangle$, $|\psi'_{2,1}\rangle, \ldots, |\psi'_{2,k}\rangle$, and $|\psi'_{3,1}\rangle, \ldots, |\psi'_{3,r}\rangle$ of $2q_{\mathcal{M}}(|x|)$ qubits, which are set in the quantum registers $(\mathsf{R}_{1,1}, \mathsf{S}_{1,1}), \ldots, (\mathsf{R}_{1,k}, \mathsf{S}_{1,k})$, $(\mathsf{R}_{2,1}, \mathsf{S}_{2,1}), \ldots, (\mathsf{R}_{2,k}, \mathsf{S}_{2,k})$, and $(\mathsf{R}_{3,1}, \mathsf{S}_{3,1}), \ldots, (\mathsf{R}_{3,r}, \mathsf{S}_{3,r})$, respectively, and let $|\psi'_1\rangle = |\psi'_{1,1}\rangle \otimes \cdots \otimes |\psi'_{1,k}\rangle$ and $|\psi'_2\rangle = |\psi'_{2,1}\rangle \otimes \cdots \otimes |\psi'_{2,k}\rangle$. Let $\rho = \rho_1 \otimes \cdots \otimes \rho_k$ and $\sigma = \sigma_1 \otimes \cdots \otimes \sigma_k$, where $\rho_j = \text{tr}_{\mathcal{R}_{1,j}} |\psi'_{1,j}\rangle\langle\psi'_{1,j}|$ and $\sigma_j = \text{tr}_{\mathcal{R}_{2,j}} |\psi'_{2,j}\rangle\langle\psi'_{2,j}|$ for each $1 \leq j \leq k$. Note that, if $\text{tr}(\rho\sigma) > 1 - \frac{\delta}{5}$, there exist pure states $|\xi'_{1,j}\rangle \in \mathcal{R}_{1,j}$, $|\xi'_{2,j}\rangle \in \mathcal{R}_{2,j}$, $|\eta'_{1,j}\rangle \in \mathcal{S}_{1,j}$, and $|\eta'_{2,j}\rangle \in \mathcal{S}_{2,j}$ for each $1 \leq j \leq k$ such that the states $|\phi'_1\rangle = |\xi'_{1,1}\rangle \otimes |\eta'_{1,1}\rangle \otimes \cdots \otimes |\xi'_{1,k}\rangle \otimes |\eta'_{1,k}\rangle$ and $|\phi'_2\rangle = |\xi'_{2,1}\rangle \otimes |\eta'_{2,1}\rangle \otimes \cdots \otimes |\xi'_{2,k}\rangle \otimes |\eta'_{2,k}\rangle$ satisfy that $F\bigl(|\phi'_1\rangle\langle\phi'_1|, |\psi'_1\rangle\langle\psi'_1|\bigr) > \sqrt{1 - \frac{\delta}{5}}$ and $F\bigl(|\phi'_2\rangle\langle\phi'_2|, |\psi'_2\rangle\langle\psi'_2|\bigr) > \sqrt{1 - \frac{\delta}{5}}$. Now the claim follows from the argument almost parallel to the proof of Proposition 11. □

Now Theorem 4 can be proved by using the transformation in Lemma 10 repeatedly.

Proof of Theorem 4. From Corollary 8, we have that $\text{QMA}(k, c, s) \subseteq \text{QMA}\bigl(k, 1 - 2^{-p}, 1 - \frac{c-s}{2}\bigr)$ for any function $p \in \text{poly}$. Now we repeatedly apply the transformation in Lemma 10 $O(\log k)$ times, and finally we obtain a two-proof system with completeness at least $1 - 2^{-p}$ and soundness at most $1 - \frac{1}{q}$ for some function $q \in \text{poly}$.

Verifier's Protocol in $(2k+r)$-Proof System

1. For each $(i,j) \in \{(1,1),\dots,(1,k),(2,1),\dots,(2,k),(3,1),\dots,(3,r)\}$, receive the quantum proof $|\psi_{i,j}\rangle$ in $(\mathsf{R}_{i,j},\mathsf{S}_{i,j})$. Reject if any of the qubits in $\mathsf{S}_{3,j}$ contains 1, for $1 \le j \le r$.
2. Do one of the following two tests uniformly at random.

   2.1 (SEPARABILITY TEST)
   Perform the controlled-swap test over $(\mathsf{S}_{1,1},\dots,\mathsf{S}_{1,k})$ and $(\mathsf{S}_{2,1},\dots,\mathsf{S}_{2,k})$ using B as a control qubit. That is, perform the following:

   2.1.1 Apply the Hadamard transformation H to B.

   2.1.2 Apply the controlled-swap operator to $(\mathsf{S}_{1,1},\dots,\mathsf{S}_{1,k})$ and $(\mathsf{S}_{2,1},\dots,\mathsf{S}_{2,k})$ using B as a control qubit.

   2.1.3 Apply the Hadamard transformation H to B. Accept if B contains 0, and reject otherwise.

   2.2 (SIMULATION TEST)
   Apply $V(x)$ to the qubits in $(\mathsf{V},\mathsf{R}_{1,1},\dots,\mathsf{R}_{1,k},\mathsf{R}_{2,1},\dots,\mathsf{R}_{2,k},\mathsf{S}_{1,1},\dots,\mathsf{S}_{1,k},\mathsf{R}_{3,1},\dots,\mathsf{R}_{3,r})$. Accept iff the result corresponds to the accepting computation of the original quantum verifier.

Figure 3: Verifier's protocol in $(2k+r)$-proof system.

Here the function q is determined only by k and $c-s$ and independent of p, as the soundness after each application of the transformation in Lemma 10 only depends on the soundness of the original system before the application. Thus, for any p, the same soundness $1-\frac{1}{q}$ is satisfied. Finally, note that the size of the circuit of the verifier after each application of the transformation in Lemma 10 is at most some constant times that of the original verifier plus an amount bounded by a polynomial in the input length. Thus, given a description of the circuit of the verifier in the original k-proof system, one can compute in time polynomial in the input length a description of the circuit of the verifier in the resulting two-proof system, and the theorem follows. □

5 Cases with Perfect Soundness

This section focuses on the quantum multi-proof Merlin-Arthur proof systems of perfect soundness. It is proved that multiple quantum proofs do not increase the verification power in the case of perfect soundness, which also gives a connection between two existing concepts of "quantum nondeterminism". Formally, the following is proved.

Theorem 12. *For any functions $k \in \mathrm{poly}$ and $c\colon \mathbb{Z}^+ \to [0,1]$,*

$$\mathrm{QMA}(k,c,0) = \mathrm{QMA}(1,c,0).$$

Proof. The inclusion $\mathrm{QMA}(k,c,0) \supseteq \mathrm{QMA}(1,c,0)$ is trivial, and we show the other inclusion.

Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem in $\mathrm{QMA}(k,c,0)$. Given a $\mathrm{QMA}(k,c,0)$ proof system for A, we construct a $\mathrm{QMA}(1,c,0)$ proof system for A in the following way.

Let V be a quantum verifier of the $\mathrm{QMA}(k,c,0)$ proof system. For every input x, assume that each quantum proof V receives is of size $q(|x|)$, for some function $q \in \mathrm{poly}$. Our new quantum verifier W in the $\mathrm{QMA}(1,c,0)$ proof system receives one quantum proof of size $k(|x|)q(|x|)$ and simulates V with this quantum proof.

The completeness is clearly at least c.

NQP Simulation of NQMA Proof System

1. Apply the Hadamard transformation H to every qubit in S_1.
2. Copy the contents of S_1 to those of S_2.
3. Apply $V(x)$ to the pair of quantum registers $(\mathsf{R}, \mathsf{S}_1)$. Accept if the contents of $(\mathsf{R}, \mathsf{S}_1)$ make the original verifier accept.

Figure 4: NQP simulation of an NQMA proof system.

For the soundness, assume that the input x is in A_{no}. Let $|\phi\rangle$ be any quantum proof of size $k(|x|)q(|x|)$. Let e_i be the lexicographically ith string in $\Sigma^{k(|x|)q(|x|)}$. Note that, for every i, the original verifier V never accepts x when the $k(|x|)$ quantum proofs he receives form the state $|e_i\rangle$. Since any $|\phi\rangle$ is expressed as a linear combination of these $|e_i\rangle$, it follows that W rejects x with certainty. □

Let $\mathrm{EQMA}(k) = \mathrm{QMA}(k, 1, 0)$ and $\mathrm{RQMA}(k) = \mathrm{QMA}\big(k, \frac{1}{2}, 0\big)$ for every k. Theorem 12 implies that $\mathrm{EQMA}(k) = \mathrm{EQMA}(1)$ and $\mathrm{RQMA}(k) = \mathrm{RQMA}(1)$. Furthermore, one can consider the complexity class $\mathrm{NQMA}(k)$ that combines two existing concepts of "quantum nondeterminism", $\mathrm{QMA}(k)$ and NQP.

Definition 13. A problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{NQMA}(k)$ if there exists a function $c \colon \mathbb{Z}^+ \to (0, 1]$ such that A is in $\mathrm{QMA}(k, c, 0)$.

Note that $\mathrm{NQMA}(k) = \mathrm{NQMA}(1)$ is also immediate from Theorem 12. The next theorem shows that $\mathrm{NQMA}(1)$ coincides with the class NQP.

Theorem 14. $\mathrm{EQMA}(1) \subseteq \mathrm{RQMA}(1) \subseteq \mathrm{NQMA}(1) = \mathrm{NQP}$.

Proof. It is sufficient to show that $\mathrm{NQMA}(1) \subseteq \mathrm{NQP}$, since $\mathrm{EQMA}(1) \subseteq \mathrm{RQMA}(1) \subseteq \mathrm{NQMA}(1)$ and $\mathrm{NQMA}(1) \supseteq \mathrm{NQP}$ hold obviously.

Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem in $\mathrm{NQMA}(1)$. Given an $\mathrm{NQMA}(1)$ proof system for A, we construct an NQP algorithm for A.

Let V be the quantum verifier of the $\mathrm{NQMA}(1)$ proof system. For every input x, suppose that V uses $q_{\mathcal{V}}(|x|)$ private qubits and receives a quantum proof of $q_{\mathcal{M}}(|x|)$ qubits, for some functions $q_{\mathcal{V}}, q_{\mathcal{M}} \in \mathrm{poly}$. Let $V(x)$ be the unitary transformation V applies. In the NQP algorithm for A, we prepare quantum registers R, S_1, and S_2, where R consists of $q_{\mathcal{V}}(|x|)$ qubits and each S_i consists of $q_{\mathcal{M}}(|x|)$ qubits. All the qubits in R, S_1, and S_2 are initialized to state $|0\rangle$. The precise algorithm is described in Figure 4.

For the completeness, suppose that the input x is in A_{yes}. In the original $\mathrm{NQMA}(1)$ proof system for A, there exists a quantum proof $|\phi\rangle$ of size $q_{\mathcal{M}}(|x|)$ that causes V to accept x with non-zero probability. Suppose that V never accepts x with any given quantum proof $|e_i\rangle$ for $1 \leq i \leq 2^{q_{\mathcal{M}}(|x|)}$, where e_i is the lexicographically ith string in $\Sigma^{q_{\mathcal{M}}(|x|)}$. Then with a similar argument to the proof of Theorem 12, V never accepts x with any given quantum proof $|\phi\rangle$ of size $q_{\mathcal{M}}(|x|)$, which contradicts the assumption. Thus there is at least one $|e_i\rangle$ that causes V to accept x with non-zero probability. Hence, in the algorithm in Figure 4, the probability of acceptance must be non-zero, since it simulates with probability $2^{-q_{\mathcal{M}}(|x|)}$ the case where V is given a proof $|e_i\rangle$ for every i.

Now for the soundness, suppose that the input x is in A_{no}. In the original $\mathrm{NQMA}(1)$ proof system for A, no matter which quantum proof $|\phi\rangle$ of size $q_{\mathcal{M}}(|x|)$ is given, V never accepts x. Hence, in the algorithm in Figure 4, the probability of acceptance is zero and the soundness follows. □

Now the following characterization of NQP is immediate.

Theorem 15. $\mathrm{NQP} = \bigcup_{c \colon \mathbb{Z}^+ \to (0,1]} \mathrm{QMA}(1, c, 0)$.

6 Impossibility of Excluding Entangled Quantum Proofs

This section shows that there is no POVM measurement that determines whether a given unknown state is in a tensor product form or maximally entangled. This especially shows that an attempt of ruling out any quantum proof far from states of a tensor product of two quantum proofs at the beginning of verification does not work when simulating a two-proof system by a single-proof system.

Suppose that there is a quantum subroutine that answers which of the following (a) and (b) is true for a given proof $|\Psi\rangle \in \mathcal{H}^{\otimes 2}$ of $2n$ qubits, where $\mathcal{H}$ is the Hilbert space consisting of n qubits:

(a) $|\Psi\rangle\langle\Psi|$ is in $\mathsf{H}_0 = \bigl\{|\Psi_0\rangle\langle\Psi_0|\colon |\Psi_0\rangle \in \mathcal{H}^{\otimes 2},\ \exists|\phi\rangle, |\psi\rangle \in \mathcal{H},\ |\Psi_0\rangle = |\phi\rangle \otimes |\psi\rangle\bigr\}$,

(b) $|\Psi\rangle\langle\Psi|$ is in $\mathsf{H}_1^{\varepsilon} = \bigl\{|\Psi_1\rangle\langle\Psi_1|\colon |\Psi_1\rangle \in \mathcal{H}^{\otimes 2},\ \max_{|\phi\rangle,|\psi\rangle\in\mathcal{H}} F(|\Psi_1\rangle\langle\Psi_1|, |\phi\rangle\langle\phi| \otimes |\psi\rangle\langle\psi|) \le 1-\varepsilon\bigr\}$.

For a proof $|\Psi\rangle$ that does not satisfy (a) nor (b), this subroutine may answer (a) or (b) arbitrarily. The rest of this section proves that this kind of subroutines cannot be realized by any physical method. In fact, we prove a stronger statement that the set of states in a tensor product form cannot be distinguished even from the set of maximally entangled states by any physical operation. Here, following Ref. [14], we say that the n-qubit state $\rho = |\Psi\rangle\langle\Psi|$ is *maximally entangled* if $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \sum_{i=1}^{d} \alpha_i |e_i\rangle \otimes |f_i\rangle, \quad |\alpha_i|^2 = \frac{1}{d},$$

where $d = 2^n$ is the dimension of $\mathcal{H}$ and $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ are orthonormal bases of $\mathcal{H}$. Among all states, maximally entangled states are farthest away from states in a tensor product form, and

$$\min_{|\Psi\rangle\in\mathcal{H}^{\otimes 2}} \max_{|\phi\rangle,|\psi\rangle\in\mathcal{H}} F(|\Psi\rangle\langle\Psi|, |\phi\rangle\langle\phi| \otimes |\psi\rangle\langle\psi|) = \frac{1}{\sqrt{d}} = 2^{-\frac{n}{2}}$$

is achieved by maximally entangled states.

Theorem 16. *Suppose that one of the following two is true for a given proof $|\Psi\rangle \in \mathcal{H}^{\otimes 2}$ of $2n$ qubits:*

(a) $|\Psi\rangle\langle\Psi|$ *is in* $\mathsf{H}_0 = \bigl\{|\Psi_0\rangle\langle\Psi_0|\colon |\Psi_0\rangle \in \mathcal{H}^{\otimes 2},\ \exists|\phi\rangle, |\psi\rangle \in \mathcal{H},\ |\Psi_0\rangle = |\phi\rangle \otimes |\psi\rangle\bigr\}$,

(b) $|\Psi\rangle\langle\Psi|$ *is in* $\mathsf{H}_1 = \bigl\{|\Psi_1\rangle\langle\Psi_1|\colon |\Psi_1\rangle \in \mathcal{H}^{\otimes 2} \text{ is maximally entangled}\bigr\}$.

Then, in determining which of (a) and (b) is true, no POVM measurement is better than the trivial strategy in which one guesses at random without any operation at all.

Proof. Let $\boldsymbol{M} = \{M_0, M_1\}$ be a POVM on $\mathcal{H}^{\otimes 2}$. With $\boldsymbol{M}$ we conclude $|\Psi\rangle\langle\Psi| \in \mathsf{H}_i$ if $\boldsymbol{M}$ results in i, $i \in \{0,1\}$. Let $\mathrm{P}^{\boldsymbol{M}}_{i\to j}(|\Psi\rangle\langle\Psi|)$ denote the probability that $|\Psi\rangle\langle\Psi| \in \mathsf{H}_j$ is concluded by $\boldsymbol{M}$ while $|\Psi\rangle\langle\Psi| \in \mathsf{H}_i$ is true. We want to find the measurement that minimizes $\mathrm{P}^{\boldsymbol{M}}_{0\to 1}(|\Psi\rangle\langle\Psi|)$ keeping the other side of error small enough. More precisely, we consider $\mathcal{E}$ defined and bounded as follows.

$$\begin{aligned}
\mathcal{E} &\overset{\text{def}}{=} \min_{\boldsymbol{M}} \Bigl\{\max_{\rho\in\mathsf{H}_0} \mathrm{P}^{\boldsymbol{M}}_{0\to 1}(\rho)\colon \max_{\rho\in\mathsf{H}_1} \mathrm{P}^{\boldsymbol{M}}_{1\to 0}(\rho) \le \delta\Bigr\} \\
&\ge \min_{\boldsymbol{M}} \left\{\int_{\rho\in\mathsf{H}_0} \mathrm{P}^{\boldsymbol{M}}_{0\to 1}(\rho)\mu_0(\mathrm{d}\rho)\colon \int_{\rho\in\mathsf{H}_1} \mathrm{P}^{\boldsymbol{M}}_{1\to 0}(\rho)\mu_1(\mathrm{d}\rho) \le \delta\right\} \\
&= \min_{\boldsymbol{M}} \left\{\mathrm{P}^{\boldsymbol{M}}_{0\to 1}\left(\int_{\rho\in\mathsf{H}_0} \rho\mu_0(\mathrm{d}\rho)\right) : \mathrm{P}^{\boldsymbol{M}}_{1\to 0}\left(\int_{\rho\in\mathsf{H}_1} \rho\mu_1(\mathrm{d}\rho)\right) \le \delta\right\},
\end{aligned}$$

where each μ_i is an arbitrary probability measure in H_i. It follows that $\mathcal{E}$ is larger than the error probability in distinguishing $\int_{\rho \in \mathsf{H}_0} \rho \mu_0(\mathrm{d}\rho)$ from $\int_{\rho \in \mathsf{H}_1} \rho \mu_1(\mathrm{d}\rho)$.

Take μ_0 as a uniform distribution over the set $\{|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|\}_{1 \leq i,j \leq d}$, that is, $\mu_0(|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|) = \frac{1}{d^2}$ for each i and j, where $\{|e_i\rangle\}$ is an orthonormal basis of $\mathcal{H}$, and take μ_1 as a uniform distribution over the set $\{|g_{k,l}\rangle\langle g_{k,l}|\}_{1 \leq k,l \leq d}$, that is, $\mu_1(|g_{k,l}\rangle\langle g_{k,l}|) = \frac{1}{d^2}$ for each k and l, where

$$|g_{k,l}\rangle = \frac{1}{d} \sum_{j=1}^{d} \bigl(e^{2\pi\sqrt{-1}\frac{jk}{d}} |e_j\rangle \otimes |e_{(j+l) \bmod d}\rangle \bigr).$$

This $\{|g_{k,l}\rangle\}$ forms an orthonormal basis of $\mathcal{H}^{\otimes 2}$ [15], and thus

$$\int_{\rho \in \mathsf{H}_0} \rho \mu_0(\mathrm{d}\rho) = \int_{\rho \in \mathsf{H}_1} \rho \mu_1(\mathrm{d}\rho) = \frac{1}{d^2} I_{\mathcal{H}^{\otimes 2}}.$$

Hence we have the assertion. □

Now the following corollary is immediate from Theorem 16.

Corollary 17. *Suppose one of the following two is true for the proof $|\Psi\rangle \in \mathcal{H}^{\otimes 2}$ of $2n$ qubits:*

(a) $|\Psi\rangle\langle\Psi|$ *is in* $\mathsf{H}_0 = \bigl\{ |\Psi_0\rangle\langle\Psi_0| \colon |\Psi_0\rangle \in \mathcal{H}^{\otimes 2},\ \exists |\phi\rangle, |\psi\rangle \in \mathcal{H},\ |\Psi_0\rangle = |\phi\rangle \otimes |\psi\rangle \bigr\}$,

(b) $|\Psi\rangle\langle\Psi|$ *is in* $\mathsf{H}_1^{\varepsilon} = \bigl\{ |\Psi_1\rangle\langle\Psi_1| \colon |\Psi_1\rangle \in \mathcal{H}^{\otimes 2},\ \max_{|\phi\rangle, |\psi\rangle \in \mathcal{H}} F(|\Psi_1\rangle\langle\Psi_1|, |\phi\rangle\langle\phi| \otimes |\psi\rangle\langle\psi|) \leq 1 - \varepsilon \bigr\}$.

Then, for any $0 \leq \varepsilon \leq 1 - 2^{-\frac{n}{2}}$, in determining which of (a) and (b) is true, no POVM measurement is better than the trivial strategy in which one guesses at random without any operation at all.

7 Conclusions

This paper introduced the multi-proof version of quantum Merlin-Arthur proof systems. To investigate the possibility that multi-proof quantum Merlin-Arthur proof systems collapse to standard single-proof ones, this paper proved several basic properties like a way of reducing the number of proofs to two while keeping the two-sided bounded-error property, and a necessary and sufficient condition under which the number of quantum proofs is reducible to two. However, the central question of whether multiple quantum proofs are indeed more helpful to Arthur still remains open. The authors hope that this paper sheds light on new features on quantum Merlin-Arthur proof systems and entanglement theory, and more widely on quantum computational complexity and quantum information theory.

Acknowledgements

The authors are grateful to John Watrous for providing us with an unpublished proof of QMA ⊆ PP, which was shown jointly by Alexei Yu. Kitaev and John Watrous. Lemma 7 was found during a discussion between HK and John Watrous, and HK is grateful to him. HK thanks Richard Cleve and Lance Fortnow for their helpful comments. Finally, the authors thank anonymous referees who provided many suggestions for improving this paper.

References

[1] Scott Aaronson. QMA/qpoly ⊆ PSPACE/poly: De-Merlinizing quantum protocols. In *Twenty-First Annual IEEE Conference on Computational Complexity*, pages 261–273, 2006.

[2] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5:1–42 (Article 1), 2009.

[3] Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3:129–157 (Article 7), 2007.

[4] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[5] Dorit Aharonov, Daniel Gottesman, Sandy Irani, and Julia Kempe. The power of quantum systems on a line. *Communications in Mathematical Physics*, 287(1):41–65, 2009.

[6] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[7] Dorit Aharonov and Oded Regev. A lattice problem in quantum NP. In *44th Annual Symposium on Foundations of Computer Science*, pages 210–219, 2003.

[8] Vikraman Arvind and Johannes Köbler. On pseudorandomness and resource-bounded measure. *Theoretical Computer Science*, 255(1–2):205–221, 2001.

[9] László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[10] László Babai. Bounded round interactive proofs in finite groups. *SIAM Journal on Discrete Mathematics*, 5(1):88–111, 1992.

[11] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[12] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3(4):307–318, 1993.

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

[14] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046–2052, 1996.

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

[16] Hugue Blier and Alain Tapp. All languages in NP have very short quantum proofs. In *The Third International Conference on Quantum, Nano and Micro Technologies, ICQNM 2009*, pages 34–37, 2009.

[17] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[18] Harry Buhrman and Dieter van Melkebeek. Hard sets are hard to find. *Journal of Computer and System Sciences*, 59(2):327–345, 1999.

[19] Harry Buhrman, Dieter van Melkebeek, Kenneth W. Regan, D. Sivakumar, and Martin Strauss. A generalization of resource-bounded measure, with application to the BPP vs. EXP problem. *SIAM Journal on Computing*, 30(2):576–601, 2000.

[20] Shimon Even, Alan L. Selman, and Yacov Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.

[21] Stephen Fenner, Frederic Green, Steven Homer, and Randall Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proceedings: Mathematical, Physical and Engineering Sciences*, 455(1991):3953–3966, 1999.

[22] Lance Fortnow and John Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[23] Oded Goldreich and David Zuckerman. Another proof that BPP subseteq PH (and more). Electronic Colloquium on Computational Complexity, Report TR97-045, 1997.

[24] Alexander S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*, volume 1 of *North-Holland Series in Statistics and Probability*. North-Holland Publishing Company, 1982.

[25] Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. In search of an easy witness: exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002.

[26] Dominik Janzing, Pawel Wocjan, and Thomas Beth. Non-identity check is QMA-complete. *International Journal of Quantum Information*, 3(3):463–473, 2005.

[27] Richard Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

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

[29] Julia Kempe and Oded Regev. 3-local Hamiltonian is QMA-complete. *Quantum Information and Computation*, 3(3):258–264, 2003.

[30] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.

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

[32] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[33] E. Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996.

[34] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[35] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198, 2003.

[36] Yi-Kai Liu. Consistency of local density matrices is QMA-complete. In *Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques, 9th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006 and 10th International Workshop on Randomization and Computation, RANDOM 2006*, volume 4110 of *Lecture Notes in Computer Science*, pages 450–461, 2006.

[37] Yi-Kai Liu. *The Complexity of the Consistency and N-representability Problems for Quantum States*. PhD thesis, University of California – San Diego, 2007.

[38] Yi-Kai Liu, Matthias Christandl, and F. Verstraete. Quantum computational complexity of the N-representability problem: QMA complete. *Physical Review Letters*, 98(11):110503, 2007.

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

[40] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003.

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

[42] Masanao Ozawa. Quantum measuring processes of continuous observables. *Journal of Mathematical Physics*, 25(1):79–87, 1984.

[43] Ran Raz and Amir Shpilka. On the power of quantum proofs. In *Nineteenth Annual IEEE Conference on Computational Complexity*, pages 260–274, 2004.

[44] Alexander Russell and Ravi Sundaram. Symmetric alternation captures BPP. *Computational Complexity*, 7(2):152–162, 1998.

[45] Rahul Santhanam. Circuit lower bounds for Merlin-Arthur classes. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 275–283, 2007.

[46] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(1):012310, 2002.

[47] Nikolai K. Vereshchagin. On the power of PP. In *Proceedings, Structure in Complexity Theory, Seventh Annual Conference*, pages 138–143, 1992.

[48] John Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual Symposium on Foundations of Computer Science*, pages 537–546, 2000.

[49] Pawel Wocjan, Dominik Janzing, and Thomas Beth. Two QCMA-complete problems. *Quantum Information and Computation*, 3(6):635–643, 2003.

[50] Ronald de Wolf. Nondeterministic quantum query and communication complexities. *SIAM Journal on Computing*, 32(3):681–699, 2003.

[51] Tomoyuki Yamakami and Andrew C. Yao. $\mathrm{NQP}_{\mathbb{C}} = \mathrm{co}\text{-}\mathrm{C}_{=}\mathrm{P}$. *Information Processing Letters*, 71(2):63–69, 1999.