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

Hirotada Kobayashi[*†] hirotada@qci.jst.go.jp
Keiji Matsumoto[‡*] keiji@nii.ac.jp
Tomoyuki Yamakami[§] yamakami@site.uottawa.ca

[*]Quantum Computation and Information Project
Exploratory Research for Advanced Technology
Japan Science and Technology Corporation
5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

[†]Department of Information Science
Graduate School of Science
The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

[‡]Foundations of Information Research Division
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

[§]School of Information Technology and Engineering
University of Ottawa
150 Louis Pasteur, P.O. Box 450, Stn A Ottawa, Ontario, Canada K1N 6N5

6 June 2003

Abstract

Quantum Merlin-Arthur proof systems are a weak form of quantum interactive proof systems, where mighty Merlin as a prover presents a proof in a pure quantum state and Arthur as a verifier performs polynomial-time quantum computation to verify its correctness with high success probability. For a more general treatment, this paper considers quantum "multiple-Merlin"-Arthur proof systems in which Arthur uses multiple quantum proofs unentangled each other for his verification. Although classical multi-proof systems are easily shown to be essentially equivalent to classical single-proof systems, it is unclear whether quantum multi-proof systems collapse to quantum single-proof systems. This paper investigates the possibility that quantum multi-proof systems collapse to quantum single-proof systems, and shows that (i) a necessary and sufficient condition under which the number of quantum proofs is reducible to two and (ii) using multiple quantum proofs does not increase the power of quantum Merlin-Arthur proof systems in the case of perfect soundness. Our proof for the latter result also gives a new characterization of the class NQP, which bridges two existing concepts of "quantum nondeterminism". It is also shown that (iii) there is a relativized world in which co-NP (actually co-UP) does not have quantum Merlin-Arthur proof systems even with multiple quantum proofs.

1 Introduction

Babai [3] introduced Merlin-Arthur proof systems (or Merlin-Arthur games as originally called), which can be viewed as a weak form of interactive proof systems in which powerful Merlin, who is a prover, presents a proof and Arthur, who is a verifier, probabilistically verifies its correctness with high success probability. The class of languages having Merlin-Arthur proof systems is denoted by MA, and has played important roles in computational complexity theory [3, 5, 4] (also see [13] for history).

A quantum analogue of MA was first discussed by Knill [28] and studied intensively by Kitaev [25], Watrous [34], and a number of very recent works [24, 35, 21, 22, 36]. 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. However, all the previous works only consider the model in which Arthur receives a single quantum proof, and no discussions are done so far on the model in which Arthur receives *multiple* quantum proofs unentangled each other.

Classically, multiple proofs can be concatenated into a long single proof, and thus, there is no advantage to use multiple proofs. However, it is unclear whether using multiple quantum proofs is computationally equivalent to using a single quantum proof, because knowing that a given proof is a tensor product of some unentangled quantum states might be advantageous to Arthur and might make significant difference. For example, in the case of two quantum proofs versus one, consider the following most straightforward Arthur's simulation of two quantum proofs by a single quantum proof: given a single quantum proof that is expected to be a tensor product of two unentangled quantum states, Arthur first runs some pre-processing to rule out any quantum proof far from states of a tensor product of two unentangled quantum states, and then performs the verification procedure for two-proof systems. It turns out that this most straightforward method does not work well, since there is no positive operator value measurement (POVM) that determines whether a given unknown state is in a tensor product form or even maximally entangled, as is shown in Section 7. Other fact is that the unpublished proof by Kitaev and Watrous for the upper bound PP of the class QMA of languages having single-proof quantum Merlin-Arthur proof systems (and even the proof of $\mathrm{QMA} \subseteq \mathrm{PSPACE}$ [25, 26]) no longer works well for the multi-proof cases with the most straightforward modification. Also, the existing proofs that parallel repetition of a single-proof protocol reduces the error probability to be arbitrarily small [27, 34, 26] cannot be applied to the multi-proof cases. Of course, these arguments do not imply that using multiple quantum proofs is more powerful from the complexity theoretical viewpoint than using only a single quantum proof. The authors believe, however, that these at least justify that it is meaningful to consider the multi-proof model of quantum Merlin-Arthur proof systems.

For this reason, this paper extends the usual 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 pure quantum states. One may think of this model as a special case of quantum multi-prover interactive proof systems discussed in [29]in which a verifier cannot ask questions to provers, and provers do not share entanglement a priori. Formally, we say that a language L has a (k, a, b)*-quantum Merlin-Arthur proof system* if there exists a polynomial-time quantum verifier V such that, for every input x of length n, (i) if $x \in L$, there exists a set of k quantum proofs which causes V to accept x with probability at least $a(n)$, and (ii) if $x \notin L$, for any set of k quantum proofs, V accepts x with probability at most $b(n)$. Let $\mathrm{QMA}(k, a, b)$ denote the class of languages having (k, a, b)-quantum Merlin-Arthur proof systems. We often abbreviate $\mathrm{QMA}(k)$ for $\mathrm{QMA}(k, 2/3, 1/3)$ for brevity throughout this paper.

This paper first shows a condition under which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$. Our condition is related to the possibility of amplifying success probabilities without increasing the number of quantum proofs. More formally, we have $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ for every k if $\mathrm{QMA}(k, a, b)$ coincides with $\mathrm{QMA}(k, 2/3, 1/3)$ for every k and any two-sided bounded error probabilities (a, b). Furthermore, $\mathrm{QMA}(k, a, b)$ coincides with $\mathrm{QMA}(2, 2/3, 1/3)$ for every k and any two-sided bounded error probability (a, b), if and only if $\mathrm{QMA}(k, a, b)$ coincides with $\mathrm{QMA}(k, 2/3, 1/3)$ for every k and any two-sided bounded error probability (a,b). Our proofs for these properties also imply an interesting consequence for the case of perfect completeness. Namely, $\mathrm{QMA}(k,1,b)=\mathrm{QMA}(1,1,1/2)$ for every fixed positive integer $k\geq 2$ and any bounded error probability b, if and only if $\mathrm{QMA}(2,1,b)=\mathrm{QMA}(1,1,b)$ for any bounded error probability b.

Next, for the case of perfect soundness, it is shown that $\mathrm{QMA}(k,a,0)=\mathrm{QMA}(1,a,0)$ for every k and any error probability a. With further analyses, the class NQP, which is the class resulting from another concept of "quantum nondeterminism" introduced by Adleman, DeMarrais, and Huang [1] and discussed by a number of works [15, 14, 38], is characterized by the union of $\mathrm{QMA}(1,a,0)$ for all error probability functions a. This bridges between two existing concepts of "quantum nondeterminism".

Finally, to see a limitation of $\mathrm{QMA}(k)$, this paper exhibits a relativized world where $\mathrm{QMA}(k)$ is not as powerful as the polynomial-time hierarchy. Earlier, Fortnow and Sipser [17] built an oracle relative to which IP does not include co-NP (Fortnow, Rompel, and Sipser [16] extended this to an oracle relative to which even MIP does not include co-NP). This paper constructs a relativized world in which $\mathrm{QMA}(k)$ does not contain co-NP (actually we show an oracle A relative to which $\text{co-UP}^A \not\subseteq \mathrm{QMA}(k)^A$ for every k). The construction uses a technique, so-called a block sensitivity method, developed mostly for the black-box computation model. As an immediate consequence, we have that, for every k, there exists a relativized world in which none of BQP, $\mathrm{QMA}(k)$, and co-$\mathrm{QMA}(k)$ coincides with each other.

The remainder of this paper is organized as follows. In Section 2 we give a brief review for several basic notions of quantum computation and information theory used in this paper. In Section 3 we formally define the multi-proof model of quantum Merlin-Arthur proof systems. In Section 4 we show a condition under which $\mathrm{QMA}(k)=\mathrm{QMA}(2)$. In Section 5 we focus on the one-sided bounded error cases. In Section 6 we exhibits an oracle relative to which $\mathrm{QMA}(k)$ does not contain co-UP. In Section 7 we show that there is no POVM that determines whether a given unknown state is in a tensor product form or maximally entangled. Finally, we conclude with Section 8 which summarizes this paper.

2 Preliminaries

2.1 Quantum Basics

A *pure quantum state*, or *pure state* in short, is a unit-norm vector $|\psi\rangle$ in the Hilbert space $\mathcal{H}$. A *mixed state* is a series $(p_i,|\psi_i\rangle)$ such that $\sum_i p_i=1$, $0\leq p_i\leq 1$, and $|\psi_i\rangle\in\mathcal{H}$ for each i. 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 matrix* $\rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|$. Any density matrix is positive semidefinite and has trace 1. It should be noted that different probabilistic mixtures of pure states can yield mixed states with the identical density matrix. It is also noted that there is no physical method (i.e., no measurement) to distinguish mixed states with the identical density matrix. Therefore, density matrices give complete descriptions of quantum states, and thus we may use the term "density matrix" to indicate the corresponding mixed state.

Given a density matrix ρ over Hilbert space $\mathcal{H}\otimes\mathcal{K}$, the quantum state after *tracing out* $\mathcal{K}$ is a density matrix over $\mathcal{H}$ defined as $\mathrm{tr}_{\mathcal{K}}\rho=\sum_{i=1}^{d}(I_{\mathcal{H}}\otimes\langle e_i|)\rho(I_{\mathcal{H}}\otimes|e_i\rangle)$ for any orthonormal basis $\{|e_1\rangle,\ldots,|e_d\rangle\}$ of $\mathcal{K}$, where d is the dimension of $\mathcal{K}$ and $I_{\mathcal{H}}$ is the identity operator over $\mathcal{H}$. For any mixed state with its density matrix ρ over $\mathcal{H}$, there is a pure state $|\psi\rangle$ in $\mathcal{H}\otimes\mathcal{K}$ for the Hilbert space $\mathcal{K}$ of $\dim(\mathcal{K})=\dim(\mathcal{H})$ such that $|\psi\rangle$ is a *purification* of ρ, that is, $\mathrm{tr}_{\mathcal{K}}|\psi\rangle\langle\psi|=\rho$.

A *positive operator valued measure (POVM)* is defined to be a set $\boldsymbol{M}=\{M_1,\ldots,M_k\}$ of nonnegative Hermitian operators such that $\sum_{i=1}^{k}M_i=I$. For any POVM $\boldsymbol{M}$, there is a quantum mechanical measurement such that the measurement M_i results in i with probability exactly $\mathrm{tr}(M_i\rho)$. See [20, 31] for more rigorous description of quantum measurements.

The *trace norm* of a linear operator A is defined by $\|A\|_{\mathrm{tr}}=\frac{1}{2}\mathrm{tr}\sqrt{A^\dagger A}$. The *fidelity* $F(\rho,\sigma)$ between two density matrices ρ and σ is defined by $F(\rho,\sigma)=\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$. The following three are important properties on the trace norm and the fidelity.

Theorem 1 ([2]) *Let* $\boldsymbol{p}^{\boldsymbol{M}} = (p_1^{\boldsymbol{M}}, \ldots, p_m^{\boldsymbol{M}})$ *and* $\boldsymbol{q}^{\boldsymbol{M}} = (q_1^{\boldsymbol{M}}, \ldots, q_m^{\boldsymbol{M}})$ *be the probability distributions generated by a POVM* $\boldsymbol{M}$ *on mixed states with density matrices* ρ, σ*, respectively. Then, for any POVM* $\boldsymbol{M}$*,* $1/2|\boldsymbol{p}^{\boldsymbol{M}} - \boldsymbol{q}^{\boldsymbol{M}}| \leq \|\rho - \sigma\|_{\mathrm{tr}}$*, where* $|\boldsymbol{p}^{\boldsymbol{M}} - \boldsymbol{q}^{\boldsymbol{M}}| = \sum_{i=1}^{m} |p_i^{\boldsymbol{M}} - q_i^{\boldsymbol{M}}|$*.*

Theorem 2 ([18]) *For any density matrices* ρ *and* σ*,* $1 - F(\rho, \sigma) \leq \|\rho - \sigma\|_{\mathrm{tr}} \leq \sqrt{1 - (F(\rho, \sigma))^2}$*.*

Theorem 3 ([23]) *For any density matrices* ρ_1*,* ρ_2*,* σ_1*, and* σ_2*,*

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

For more detailed description, see [19, 30, 26] for instance.

2.2 Quantum Turing Machines

We use a model of multi-tape quantum Turing machines (referred to as QTMs) [10, 37, 32]. Formally, a k-tape QTM is defined as a sextuple $(Q, \Sigma_1 \times \cdots \times \Sigma_k, \Gamma_1 \times \Gamma_2 \times \cdots \times \Gamma_k, q_0, Q_f, \delta)$, where Q is a finite set of internal states including the initial state q_0 and a set Q_f of final states, each Σ_i is an input alphabet of the ith tape, each Γ_i is a tape alphabet of the ith tape including a distinguished blank symbol $\natural$ and Σ_i, and δ is a quantum transition function from $Q \times \Gamma_1 \times \cdots \times \Gamma_k$ to $\mathbb{C}^{Q \times \Gamma_1 \times \cdots \times \Gamma_k \times \{\leftarrow, \downarrow, \rightarrow\}^k}$. In this paper, it is assumed that all amplitudes used for QTMs are drawn from $\widetilde{\mathbb{C}}$, where $\widetilde{\mathbb{C}}$ is the set of complex numbers whose real part and imaginary part are approximated to within 2^{-n} by a deterministic Turing machine on input 1^n in time polynomial in n. A multi-tape QTM M is *well-formed* if its time-evolution operator U_M preserves the l_2-norm, that is, $\|U|\phi\rangle\| = \||\phi\rangle\|$ for any $|\phi\rangle$.

In this paper, we also need to consider pure quantum states as (a part of) inputs to a QTM; that is, if a pure state $|\phi\rangle$ of n qubits is an input to a QTM M, then M begins its computation with a superposition of its initial configurations, each of which constitutes s, where $s \in \{0,1\}^n$, as an input with amplitude $\langle s|\phi\rangle$. Assume that a QTM M starts with a superposition $|\phi\rangle$ of configurations and writes a qubit (called an output qubit) at the start cell of the output tape before it halts. We say that M accepts input $|\phi\rangle$ with probability p if p is the squared magnitude of the amplitude resulted from observing the start cell of the output tape in $\{|0\rangle, |1\rangle\}$ basis. In this case, we also say that M rejects input $|\phi\rangle$ with probability $1 - p$. Let $\eta_M(|\phi\rangle)$ denote the acceptance probability of M on input $|\phi\rangle$.

For more terminology, the reader should refer to [10, 19].

2.3 Quantum Circuits

A quantum circuit consists of a finite number of qubits to which a finite number of quantum gates are applied in sequence. A family $\{Q_x\}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a classical deterministic procedure that, on each input x, outputs a description of Q_x and runs in time polynomial in $n = |x|$. It is assumed that the quantum circuits in such a family are composed of gates in some reasonable, universal, finite set of quantum gates such as the Shor basis [33, 11]. 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 n. It is well-known that a polynomial-time quantum Turing machine and a polynomial-time uniformly generated family of quantum circuits are computationally equivalent. For convenience, in the subsequent sections, we often identify a circuit Q_x with the unitary operator it induces.

3 Quantum Merlin-Arthur Proof Systems

In quantum Merlin-Arthur proof systems, mighty Merlin as a prover provides a single *quantum proof* to a verifier Arthur for his verification. Here, a quantum proof is a pure state and a quantum proof of *size* s is a pure state of s qubits. Arthur uses quantum computation to verify the quantum proof in polynomial time with high success probability. There is no further interaction between Merlin and Arthur.

Here we extend this usual model of single-proof systems to the one of multi-proof systems. To be more precise, let x be any input of length n and, for each i, $1 \leq i \leq k$, let $|\phi_i\rangle$ be a quantum proof of size $q_{\mathcal{M}}(n)$, where $q_{\mathcal{M}}$ is a polynomially bounded function. These k quantum proofs are given to a verifier Arthur in the form $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_k\rangle$.

Although k, the number of quantum proofs, has been treated to be constant so far, one may think of $k\colon \mathbb{Z}^+ \to \mathbb{N}$ as a function of the input length n. Hereafter, we treat k as a function. Note that the number of quantum proofs must be bounded polynomial in n.

One can define quantum Merlin-Arthur proof systems both in terms of quantum Turing machines and in terms of quantum circuits. From the computational equivalence of polynomial-time quantum Turing machines and polynomial-time uniform quantum circuits [39], it is obvious that these two models of quantum Merlin-Arthur proof systems are equivalent in view of computational power. Here we give both of these two types of definitions. In the rest of this paper we will choose a suitable model from these two depending on the situations.

3.1 Definition Based on Quantum Turing Machines

A *quantum verifier* (or a *verifier* in short) is a multi-tape polynomial-time well-formed quantum Turing machine V with two special tapes for an input and proofs (the tape for proofs is called the *proof tape*). Let x be any input of length n. We say that V *accepts an input x with quantum proofs* $(|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_{k(n)}\rangle)$ *with probability p* if V starts with the input x and some quantum state $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_{k(n)}\rangle$ set in the proof tape and halts with the output qubit being observed to be 1 with probability exactly p.

Definition 4 *Given a polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$ and two functions $a, b\colon \mathbb{Z}^+ \to [0,1]$, a language L is in $\mathrm{QMA}(k,a,b)$ if there exist a polynomially bounded function $q_{\mathcal{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and a quantum verifier V such that, for every input x of length n,*

(i) if $x \in L$, there exists a set of quantum proofs $|\phi_1\rangle, \ldots, |\phi_{k(n)}\rangle$ of size $q_{\mathcal{M}}(n)$ that makes V accept x with probability at least $a(n)$,

(ii) if $x \notin L$, given any set of quantum proofs $|\phi_1\rangle, \ldots, |\phi_{k(n)}\rangle$ of size $q_{\mathcal{M}}(n)$, V accepts x with probability at most $b(n)$.

We say that a language L has a (k,a,b)-*quantum Merlin-Arthur proof system* if and only if L is in $\mathrm{QMA}(k,a,b)$. For simplicity, we write $\mathrm{QMA}(k)$ for $\mathrm{QMA}(k, 2/3, 1/3)$ for each k.

3.2 Definition Based on Quantum Circuits

For every input $x \in \Sigma^*$ of length $n = |x|$, consider quantum proofs $|\phi_1\rangle, \ldots, |\phi_{k(n)}\rangle$ of size $q_{\mathcal{M}}(n)$ for some polynomially bounded function $q_{\mathcal{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$.

Besides $kq_{\mathcal{M}}(n)$ qubits for the proofs, we have $q_{\mathcal{V}}(n)$ qubits called *private qubits* in our quantum circuit. Hence, the entire system of our quantum circuit consists of $q_{\mathcal{V}}(n) + kq_{\mathcal{M}}(n)$ qubits. All the private qubits are initialized to the $|0\rangle$ state, and one of the private qubits is designated as the output qubit.

A $(q_{\mathcal{V}}, q_{\mathcal{M}})$-*restricted quantum verifier* V is a polynomial-time computable mapping of the form $V\colon \Sigma^* \to \Sigma^*$. For every x of length n, $V(x)$ is a description of a polynomial-time uniformly generated quantum circuit acting on $q_{\mathcal{V}}(n) + kq_{\mathcal{M}}(n)$ qubits.

The probability that V accepts the input x is defined to be the probability that an observation of the output qubit (in the $\{|0\rangle, |1\rangle\}$ basis) yields 1, after the circuit $V(x)$ is applied to the state $|0^{q_{\mathcal{V}}(n)}\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{k(n)}\rangle$.

Definition 5 *Given a polynomially bounded function* $k\colon \mathbb{Z}^+ \to \mathbb{N}$ *and functions* $a, b\colon \mathbb{Z}^+ \to [0,1]$*, a language* L *is in* $\mathrm{QMA}(k,a,b)$ *if there exist polynomially bounded functions* $q_{\mathcal{V}}, q_{\mathcal{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ *and a* $(q_{\mathcal{V}}, q_{\mathcal{M}})$*-restricted quantum verifier* V *such that, for every* x *of length* n*,*

(i) if $x \in L$*, there exists a set of quantum proofs* $|\phi_1\rangle, \ldots, |\phi_{k(n)}\rangle$ *of size* $q_{\mathcal{M}}(n)$ *that makes* V *accept* x *with probability at least* $a(n)$*,*

(ii) if $x \notin L$*, for any set of quantum proofs* $|\phi_1\rangle, \ldots, |\phi_{k(n)}\rangle$ *of size* $q_{\mathcal{M}}(n)$*,* V *accepts* x *with probability at most* $b(n)$*.*

4 Condition under which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$

Classically, it is almost trivial to show that classical multi-proof Merlin-Arthur proof systems are essentially equivalent to single-proof ones. However, it is unclear whether quantum multi-proof Merlin-Arthur proof systems collapse to quantum single-proof systems. Moreover, it is also unclear whether there are k_1 and k_2 of $k_1 \neq k_2$ such that $\mathrm{QMA}(k_1) = \mathrm{QMA}(k_2)$. Towards settling these questions, here we give a condition under which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ for every fixed positive integer k.

Formally, we consider the following condition:

($*$) For every fixed positive integer $k \geq 2$ and any two-sided bounded error probability (a,b), $\mathrm{QMA}(k,a,b)$ coincides with $\mathrm{QMA}(k,2/3,1/3)$,

which is on the possibility of amplifying success probabilities without increasing the number of quantum proofs. Then we have the following theorem and the corollary.

Theorem 6 $\mathrm{QMA}(k,2/3,1/3) = \mathrm{QMA}(2,2/3,1/3)$ *for every fixed positive integer* $k \geq 2$*, if the condition* ($*$) *is satisfied.*

Corollary 7 $\mathrm{QMA}(k,a,b) = \mathrm{QMA}(2,2/3,1/3)$ *for every fixed positive integer* $k \geq 2$ *and any two-sided bounded error probability* (a,b)*, if and only if the condition* ($*$) *is satisfied.*

4.1 A Key Lemma for the Proofs of Theorem 6 and Corollary 7

For the proofs of Theorem 6 and Corollary 7, the following lemma plays a key role.

Lemma 8 *For any fixed positive integer* k*, any* $r \in \{0,1,2\}$*, and any two-sided bounded error probability* (a,b) *satisfying* $a > 1-(1-b)^2/10 \geq b$*,* $\mathrm{QMA}(3k+r,a,b) \subseteq \mathrm{QMA}(2k+r,a,1-(1-b)^2/10)$.

First we give proofs of Theorem 6 and Corollary 7, using Lemma 8. The proof of Lemma 8 will be given in the next subsection.

Proof of Theorem 6. Suppose that the condition ($*$) holds.

Then, for every fixed positive integer $k = 3l + r$, $r \in \{0,1,2\}$, and any two-sided bounded error probability (a,b), it is immediate from ($*$) that $\mathrm{QMA}(3l+r,a,b)$ coincides with $\mathrm{QMA}(3l+r,99/100,1/100)$.

Now, from Lemma 8, we have $\mathrm{QMA}(3l+r,99/100,1/100) \subseteq \mathrm{QMA}(2l+r,99/100,90199/100000)$, which implies that these two classes coincide with each other. Furthermore, from ($*$) we have $\mathrm{QMA}(2l+r,99/100,90199/100000) = \mathrm{QMA}(2l+r,99/100,1/100)$. Thus, $\mathrm{QMA}(3l+r,99/100,1/100)$ coincides with $\mathrm{QMA}(2l+r,99/100,1/100)$.

We repeat the above process c times for some constant $c = O(\log_{3/2} k)$, and finally we obtain that $\mathrm{QMA}(3l+r,a,b) = \mathrm{QMA}(2,99/100,1/100)$. Again from ($*$), $\mathrm{QMA}(2,99/100,1/100)$ coincides with $\mathrm{QMA}(2,a,b)$ for any two-sided bounded error probability (a,b).

Therefore we have $\mathrm{QMA}(k,2/3,1/3) = \mathrm{QMA}(2,2/3,1/3)$ for every fixed positive integer $k \geq 2$ as claimed. ☐

As for Corollary 7, the ‘if’ part is directly from the proof of Theorem 6. The ‘only if’ part is quite obvious, because that $\mathrm{QMA}(k,a,b) = \mathrm{QMA}(2,2/3,1/3)$ for every fixed positive integer $k \geq 2$ and any two-sided bounded error probability (a,b) implies $\mathrm{QMA}(k,a,b) = \mathrm{QMA}(k,2/3,1/3) = \mathrm{QMA}(2,2/3,1/3)$ for every fixed positive integer $k \geq 2$ and any two-sided bounded error probability (a,b).

4.2 Proof of Lemma 8

Now we give a proof of Lemma 8. The proof uses a special operator called *Controlled-Swap*. The Controlled-Swap operator exchanges the contents of two registers $\mathbf{S}_1$ and $\mathbf{S}_2$ if control register $\mathbf{B}$ contains 1, and does nothing if $\mathbf{B}$ contains 0.

Consider the following algorithm described below, which we call the *C-SWAP algorithm*. A similar idea was used in [12] for fingerprinting scheme.

Given a pair of mixed states ρ and σ of n qubits of the form $\rho \otimes \sigma$, prepare quantum registers $\mathbf{B}$, $\mathbf{R}_1$, and $\mathbf{R}_2$. The register $\mathbf{B}$ consists of only one qubit that is initially set to the $|0\rangle$-state, while the registers $\mathbf{R}_1$ and $\mathbf{R}_2$ consist of n qubits and ρ and σ are initially set in $\mathbf{R}_1$ and $\mathbf{R}_2$, respectively.

C-SWAP Algorithm

1. Apply the Hadamard transformation H to $\mathbf{B}$.
2. Apply the controlled-swap operator on $\mathbf{R}_1$ and $\mathbf{R}_2$ using $\mathbf{B}$ as a control qubit. That is, swap the contents of $\mathbf{R}_1$ and $\mathbf{R}_2$ if $\mathbf{B}$ contains 1, and do nothing if $\mathbf{B}$ contains 0.
3. Apply the Hadamard transformation H to $\mathbf{B}$ and accept if $\mathbf{B}$ contains 0.

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

Proof. Let $\mathcal{B}$, $\mathcal{R}_1$, and $\mathcal{R}_2$ denote the Hilbert spaces corresponding to the qubits in $\mathbf{B}$, $\mathbf{R}_1$, and $\mathbf{R}_2$, respectively. Let $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ and $\sigma = \sum_j q_j |\psi_j\rangle\langle\psi_j|$ be decompositions of ρ and σ with respect to the orthonormal bases $\{|\phi_i\rangle\}$, $\{|\psi_j\rangle\}$ of $\mathbf{R}_1$, $\mathbf{R}_2$, respectively.

We introduce the Hilbert spaces $\mathcal{S}_1 = l_2(\Sigma^n)$ and $\mathcal{S}_2 = l_2(\Sigma^n)$. Then there exist purifications $|\phi\rangle \in \mathcal{R}_1 \otimes \mathcal{S}_1$ and $|\psi\rangle \in \mathcal{R}_2 \otimes \mathcal{S}_2$ of ρ and σ, respectively, such that

$$|\phi\rangle = \sum_i \sqrt{p_i} |\phi_i\rangle|\phi_i\rangle, \quad |\psi\rangle = \sum_j \sqrt{q_j} |\psi_j\rangle|\psi_j\rangle.$$

Now consider the following pure state $|\xi\rangle \in \mathcal{B} \otimes \mathcal{R}_1 \otimes \mathcal{S}_1 \otimes \mathcal{R}_2 \otimes \mathcal{S}_2$,

$$|\xi\rangle = |0\rangle|\phi\rangle|\psi\rangle = \sum_{i,j} \sqrt{p_i q_j} |0\rangle|\phi_i\rangle|\phi_i\rangle|\psi_j\rangle|\psi_j\rangle.$$

The probability that the input pair of ρ and σ is accepted in the C-SWAP algorithm is exactly equal to the probability of acceptance when the C-SWAP algorithm is applied to $|\xi\rangle$ over the Hilbert space $\mathcal{B} \otimes \mathcal{R}_1 \otimes \mathcal{R}_2$.

If the C-SWAP algorithm is applied to $|\xi\rangle$, it is easy to see that the state $|\eta\rangle \in \mathcal{B} \otimes \mathcal{R}_1 \otimes \mathcal{S}_1 \otimes \mathcal{R}_2 \otimes \mathcal{S}_2$ before the final measurement of the output qubit is given by

$$\begin{aligned} |\eta\rangle &= \frac{1}{2}|0\rangle \otimes \left(\sum_{i,j} \sqrt{p_i q_j} \left(|\phi_i\rangle|\phi_i\rangle|\psi_j\rangle|\psi_j\rangle + |\psi_j\rangle|\phi_i\rangle|\phi_i\rangle|\psi_j\rangle \right) \right) \\ &\quad + \frac{1}{2}|1\rangle \otimes \left(\sum_{i,j} \sqrt{p_i q_j} \left(|\phi_i\rangle|\phi_i\rangle|\psi_j\rangle|\psi_j\rangle - |\psi_j\rangle|\phi_i\rangle|\phi_i\rangle|\psi_j\rangle \right) \right). \end{aligned}$$

Thus the probability of acceptance is $(1+t)/2$, where t is given by

$$t = \left(\sum_{i,j} \sqrt{p_i q_j} |\phi_i\rangle|\phi_i\rangle|\psi_j\rangle|\psi_j\rangle, \sum_{i,j} \sqrt{p_i q_j} |\psi_j\rangle|\phi_i\rangle|\phi_i\rangle|\psi_j\rangle \right) = \sum_{i,j} p_i q_j \left(|\phi_i\rangle|\psi_j\rangle, |\psi_j\rangle|\phi_i\rangle \right)$$
$$= \sum_{i,j} p_i q_j \langle\phi_i|\psi_j\rangle\langle\psi_j|\phi_i\rangle = \sum_i p_i \langle\phi_i|\sigma|\phi_i\rangle = \sum_i p_i \mathrm{tr}(\sigma|\phi_i\rangle\langle\phi_i|) = \mathrm{tr}(\rho\sigma).$$

Here $(\cdot,\cdot)$ represents the inner product. Thus we have the assertion. □

Using Proposition 9, we show Lemma 8. In the proof we use the circuit-based definition of QMA.

Proof of Lemma 8. The essence of the proof is the basis case where $k = 1$ and $r = 0$. We give the proof for this particular case below and leave the general case to the reader since it is easy to modify the following proof to the general case.

Let L be a language in $\mathrm{QMA}(3, a, b)$. Given a $\mathrm{QMA}(3, a, b)$ protocol for L, we construct a $\mathrm{QMA}\big(2, a, 1-(1-b)^2/10\big)$ protocol for L in the following way.

Let V be the quantum verifier of the original $\mathrm{QMA}(3, a, b)$ protocol. For every input x of length n, suppose that each of quantum proofs V receives consists of $q_{\mathcal{M}}(n)$ qubits and the number of private qubit of V is $q_{\mathcal{V}}(n)$. Let $V(x)$ be the unitary transformation which the original quantum verifier V applies. Our new quantum verifier W of the $\mathrm{QMA}\big(2, a, 1-(1-b)^2/10\big)$ protocol prepares quantum registers $\mathbf{R}_1$, $\mathbf{R}_2$, $\mathbf{S}_1$, and $\mathbf{S}_2$ for quantum proofs and quantum registers $\mathbf{V}$ and $\mathbf{B}$ for private computation. Each of $\mathbf{R}_i$ and $\mathbf{S}_i$ consists of $q_{\mathcal{M}}(n)$ qubits, $\mathbf{V}$ consists of $q_{\mathcal{V}}(n)$ qubits, and $\mathbf{B}$ consists of a single qubit. W receives two quantum proofs $|D_1\rangle$ and $|D_2\rangle$ of $2q_{\mathcal{M}}(n)$ qubits, which are expected to be of the form

$$|D_1\rangle = |C_1\rangle \otimes |C_3\rangle, \quad |D_2\rangle = |C_2\rangle \otimes |C_3\rangle, \tag{1}$$

where each $|C_i\rangle$ is the ith quantum proof which the original quantum verifier V receives. Of course, each $|D_i\rangle$ may not be of the form above and the first and the second $q_{\mathcal{M}}(n)$ qubits of $|D_i\rangle$ 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 $\mathbf{V}$, $\mathbf{B}$, $\mathbf{R}_i$, and $\mathbf{S}_i$, respectively. W runs the following protocol:

1. Receive the first quantum proof $|D_1\rangle$ in registers $(\mathbf{R}_1, \mathbf{S}_1)$ and the second one $|D_2\rangle$ in $(\mathbf{R}_2, \mathbf{S}_2)$.

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

   2.1 Separability test:
   Apply the C-SWAP algorithm over $\mathcal{B} \otimes \mathcal{S}_1 \otimes \mathcal{S}_2$, using quantum registers $\mathbf{B}$, $\mathbf{S}_1$, and $\mathbf{S}_2$.
   Accept if $\mathbf{B}$ contains 0, otherwise reject.

   2.2 Consistency test:
   Apply $V(x)$ over $\mathcal{V} \otimes \mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{S}_1$, using quantum registers $\mathbf{V}$, $\mathbf{R}_1$, $\mathbf{R}_2$, and $\mathbf{S}_1$.
   Accept iff the result corresponds to the acceptance computation of the original quantum verifier.

We first show the completeness property with the input $x \in L$ of length n. In the original $\mathrm{QMA}(3, a, b)$ protocol for L, there exist quantum proofs $|C_1\rangle$, $|C_2\rangle$, and $|C_3\rangle$ which cause the original quantum verifier V to accept x with probability at least $a(n)$. In the constructed protocol, let the quantum proofs $|D_1\rangle$ and $|D_2\rangle$ be of the form $|D_1\rangle = |C_1\rangle \otimes |C_3\rangle$ and $|D_2\rangle = |C_2\rangle \otimes |C_3\rangle$. Then it is obvious that the constructed quantum verifier W accepts x with probability at least $a(n)$.

For the soundness property with the input $x \notin L$ of length n, consider any pair of quantum proofs $|D_1'\rangle$ and $|D_2'\rangle$, which are set in the pairs of the quantum registers $(\mathbf{R}_1, \mathbf{S}_1)$ and $(\mathbf{R}_2, \mathbf{S}_2)$, respectively. Let $\rho = \mathrm{tr}_{\mathcal{R}_1} |D_1'\rangle\langle D_1'|$ and $\sigma = \mathrm{tr}_{\mathcal{R}_2} |D_2'\rangle\langle D_2'|$. We abbreviate $b(n)$ as b, and let $\delta = (-1 + 2b + 4\sqrt{1 + b - b^2})/5$. The reason why we set δ at this value will be clear later in the item (ii).

(i) In the case $\mathrm{tr}(\rho\sigma) \leq \delta$:
In this case the probability α that the input x is accepted in the SEPARABILITY TEST is at most

$$\alpha \leq \frac{1}{2} + \frac{\delta}{2} = \frac{2 + b + 2\sqrt{1 + b - b^2}}{5} \leq \frac{4 + 2b - b^2}{5} = 1 - \frac{(1-b)^2}{5},$$

where the second inequality is from the fact $p + q \geq 2\sqrt{pq}, p \geq 0, q \geq 0$. Thus the verifier W accepts the input x with probability at most

$$\frac{1}{2} + \frac{\alpha}{2} \leq 1 - \frac{(1-b)^2}{10}.$$

(ii) In the case $\mathrm{tr}(\rho\sigma) > \delta$:
$\mathrm{tr}(\rho\sigma) > \delta$ means that the maximum eigenvalue λ of ρ satisfies $\lambda > \delta$. Thus there exist pure states $|C'_1\rangle \in \mathcal{R}_1$ and $|C'_3\rangle \in \mathcal{S}_1$ such that

$$F(|C'_1\rangle\langle C'_1| \otimes |C'_3\rangle\langle C'_3|, |D'_1\rangle\langle D'_1|) > \sqrt{\delta},$$

since $\rho = \mathrm{tr}_{\mathcal{R}_1}|D'_1\rangle\langle D'_1|$. Similarly, the maximum eigenvalue of σ is more than δ and there exist pure states $|C'_2\rangle \in \mathcal{R}_2$ and $|C'_4\rangle \in \mathcal{S}_2$ such that

$$F(|C'_2\rangle\langle C'_2| \otimes |C'_4\rangle\langle C'_4|, |D'_2\rangle\langle D'_2|) > \sqrt{\delta}.$$

Thus, letting $|\phi\rangle = |C'_1\rangle \otimes |C'_3\rangle \otimes |C'_2\rangle \otimes |C'_4\rangle$ and $|\psi\rangle = |D'_1\rangle \otimes |D'_2\rangle$, we have from Theorem 3

$$F(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|) > \delta.$$

Therefore, from Theorem 2 we have

$$\| |\phi\rangle\langle\phi| - |\psi\rangle\langle\psi| \|_{\mathrm{tr}} \leq \sqrt{1 - (F(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|))^2} < \sqrt{1 - \delta^2}.$$

With Theorem 1, this implies that, the probability β that the input x is accepted in the CONSISTENCY TEST is bounded by

$$\beta < b + \sqrt{1 - \delta^2},$$

since given any quantum proofs $|C'_1\rangle$, $|C'_2\rangle$, and $|C'_3\rangle$ the original quantum verifier V accepts the input x with probability at most b. Noticing that δ satisfies

$$\frac{1}{2} + \frac{\delta}{2} = b + \sqrt{1 - \delta^2},$$

one can see that

$$\beta < 1 - \frac{(1-b)^2}{5}.$$

Thus the verifier W accepts the input x with probability at most

$$\frac{1}{2} + \frac{\beta}{2} < 1 - \frac{(1-b)^2}{10}.$$

□

5 One-Sided Bounded Error Cases

5.1 Cases with Perfect Completeness

First we focus on the quantum Merlin-Arthur proof systems of perfect completeness. Together with the fact that parallel repetition works well for single-proof quantum Merlin-Arthur proof systems, Lemma 8 implies the following interesting property.

Theorem 10 $\mathrm{QMA}(k,1,b) = \mathrm{QMA}(1,1,1/2)$ *for every fixed positive integer* $k \geq 2$ *and any bounded error probability* b*, if and only if* $\mathrm{QMA}(2,1,b) = \mathrm{QMA}(1,1,b)$ *for any bounded error probability* b*.*

Proof. We only show the 'if' part, since the 'only if' part is trivial.

For the case of perfect completeness, Lemma 8 implies that $\mathrm{QMA}(k,1,b_1) \subseteq \mathrm{QMA}(\lceil 2k/3 \rceil, 1, b_2)$, for any fixed positive integer k and any bounded error probability functions b_1 and b_2 satisfying $b_2 \geq 1 - (1-b_1)^2/10$.

Therefore, by applying Lemma 8 $c = O(\log_{3/2} k)$ times repeatedly, we can easily obtain that, for any fixed positive integer k and any bounded error probability b,

$$\mathrm{QMA}(k,1,b) \subseteq \mathrm{QMA}(2,1,b')$$

for some bounded error probability b'.

Now the 'if' part immediately follows from the assumption that $\mathrm{QMA}(2,1,b) = \mathrm{QMA}(1,1,b)$ for any bounded error probability b and the fact that parallel repetition works well for single-proof quantum Merlin-Arthur proof systems. □

5.2 Cases with Perfect Soundness

Now we turn to the cases with perfect soundness. It is shown that $\mathrm{QMA}(k,a,0) = \mathrm{QMA}(1,a,0)$ for every k and any error probability a. That is, multiple quantum proofs do not increase the computational power of the quantum Merlin-Arthur proof systems in the case of perfect soundness. It is also shown that NQP is characterized by the union of $\mathrm{QMA}(1,a,0)$ over all error probability functions a.

Theorem 11 *For any fixed positive integer* k *and any function* $a \colon \mathbb{Z}^+ \to (0,1]$*,* $\mathrm{QMA}(k,a,0) = \mathrm{QMA}(1,a,0)$*.*

Proof. For a language L in $\mathrm{QMA}(k,a,0)$, we show that L is also in $\mathrm{QMA}(1,a,0)$. Let V be a quantum verifier of a $(k,a,0)$-quantum Merlin-Arthur proof system for L. For every input x of length n, assume that V receives k quantum proofs of size $q(n)$,

We define a new $(1,a,0)$-quantum Merlin-Arthur proof system as follows: on input x of length n, verifier W receives one quantum proof of size $kq(n)$ and simulates V with this quantum proof.

The completeness property is clearly satisfied, and the acceptance probability of W is exactly that of V.

For the soundness property, assume that the input x of length n is not in L. Let $|D\rangle$ be any quantum proof of size $kq(n)$. Let e_i be the lexicographically ith string in $\{0,1\}^{kq(n)}$. Note that, for each i $(1 \leq i \leq 2^{kq(n)})$, V never accepts x when given a quantum proof $|e_i\rangle$. Since any $|D\rangle$ is expressed as a linear combination of all $|e_i\rangle$, $1 \leq i \leq 2^{kq(n)}$, it follows that W rejects x with certainty. □

Let $\mathrm{EQMA}(k) = \mathrm{QMA}(k,1,0)$ and $\mathrm{RQMA}(k) = \mathrm{QMA}(k,1/2,0)$ for every k. From Theorem 11 it is immediate that $\mathrm{EQMA}(k) = \mathrm{EQMA}(1)$ and $\mathrm{RQMA}(k) = \mathrm{RQMA}(1)$.

Furthermore, one can consider the complexity class $\mathrm{NQMA}(k)$ which combines two existing concepts of "quantum non-determinism", $\mathrm{QMA}(k)$ and NQP.

Definition 12 *A language* L *is in* $\mathrm{NQMA}(k)$ *iff there exists a function* $a \colon \mathbb{Z}^+ \to (0,1]$ *such that* L *is in* $\mathrm{QMA}(k,a,0)$*.*

Note that $\mathrm{NQMA}(k) = \mathrm{NQMA}(1)$ is also immediate from Theorem 11. The next theorem shows that $\mathrm{NQMA}(1)$ coincides with the class NQP.

Theorem 13 $\mathrm{EQMA}(1) \subseteq \mathrm{RQMA}(1) \subseteq \mathrm{NQMA}(1) = \mathrm{NQP}$.

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 L be a language in NQMA(1). Then there are polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and a $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V such that, for every input x of length n, (i) if $x \in L$, there exists a quantum proof $|C\rangle$ of size $q_{\mathcal{M}}(n)$ that causes V to accept x with non-zero probability, and (ii) if $x \notin L$, given any quantum proof $|C'\rangle$ of size $q_{\mathcal{M}}(n)$, V never accepts x. Let $V(x)$ be the unitary transformation V applies.

Given every input x of length n, prepare quantum registers $\mathbf{R}$, $\mathbf{S}_1$ and $\mathbf{S}_2$, where $\mathbf{R}$ consists of $q_{\mathcal{V}}(n)$ qubits and each $\mathbf{S}_i$ consists of $q_{\mathcal{M}}(n)$ qubits. Consider the following procedure:

NQP simulation of NQMA protocol

1. Apply the Hadamard transformation $H^{\otimes q_{\mathcal{M}}(n)}$ to $\mathbf{S}_1$.
2. Copy the contents of $\mathbf{S}_1$ to those of $\mathbf{S}_2$.
3. Apply $V(x)$ to the pair of quantum registers $(\mathbf{R}, \mathbf{S}_1)$ and accept if the contents of $\mathbf{R}$ correspond to those that make the original verifier V accept.

(i) In the case the input x of length n is in L:
In the original NQMA protocol for L, there exists a quantum proof $|C\rangle$ of size $q_{\mathcal{M}}(n)$ that causes V to accept x with non-zero probability. Suppose that V never accepts x on given any quantum proof $|e_j\rangle \in \{|0\rangle, |1\rangle\}^{\otimes q_{\mathcal{M}}(n)}$, $0 \leq j \leq 2^{q_{\mathcal{M}}(n)} - 1$, where e_i be the lexicographically ith string in $\{0,1\}^{q_{\mathcal{M}}(n)}$. Then with a similar argument to the proof of Theorem 11, V never accepts x on given any quantum proof $|C\rangle$ of size $q_{\mathcal{M}}(n)$, which contradicts the assumption. Thus there is at least one $|e_j\rangle \in \{|0\rangle, |1\rangle\}^{\otimes q_{\mathcal{M}}(n)}$ that causes V to accept x with non-zero probability. Hence in the procedure above the probability of acceptance is non-zero, for the procedure simulates with probability $1/2^{q_{\mathcal{M}}(n)}$ the case that V is given a proof $|e_j\rangle$ for each j.

(ii) In the case the input x of length n is not in L:
In the original NQMA protocol for L, for any given quantum proof $|C\rangle$ of size $q_{\mathcal{M}}(n)$, V never accepts x. In particular, for any quantum proof $|e_j\rangle \in \{|0\rangle, |1\rangle\}^{\otimes q_{\mathcal{M}}(n)}$ given, V never accepts x. Hence in the procedure above the probability of acceptance is zero.

□

Corollary 14 $\mathrm{NQP} = \bigcup_{a \colon \mathbb{Z}^+ \to (0,1]} \mathrm{QMA}(1, a, 0)$.

6 Relativized Separation of QMA(k)

Classically, Fortnow and Sipser [17] exhibited a relativized world in which IP does not include co-NP (and Fortnow, Rompel, and Sipser [16] extended this to an oracle relative to which even MIP does not include co-NP). This paper shows another relativized world in which QMA(k) does not include co-UP. Our proof is different from that of Fortnow and Sipser.

Theorem 15 *For every polynomial-time computable function $k \colon \mathbb{Z}^+ \to \mathbb{N}$, there exists an oracle A relative to which* $\text{co-UP}^A \not\subseteq \mathrm{QMA}(k)^A$.

The following is an immediate corollary of Theorem 15.

Corollary 16 *For every polynomial-time computable function $k\colon \mathbb{Z}^+ \to \mathbb{N}$, there exists an oracle A relative to which none of* BQP, QMA(k), *and* co-QMA(k) *coincides with each other.*

Proof. By Theorem 15, we have an oracle A such that $\text{co-NP}^A \not\subseteq \text{QMA}(k)^A$. Since $\text{co-NP}^A \subseteq \text{co-QMA}(k)^A$, it follows that $\text{co-QMA}(k)^A \not\subseteq \text{QMA}(k)^A$, and thus $\text{QMA}(k)^A \neq \text{co-QMA}(k)^A$. That $\text{BQP}^A \neq \text{QMA}(k)^A$ follows from $\text{QMA}(k)^A \neq \text{co-QMA}(k)^A$. $\square$

In what follows, we give the proof of Theorem 15. We use a so-called *block sensitivity* argument, whose quantum version was developed in [6]. Let f be any relativizable function from Σ^* to $[0,1]\cap\mathbb{R}$. If A is an oracle and $S \subseteq \Sigma^*$ be a subset of strings, then $A^{(S)}$ is the oracle satisfying that, for every y, $A(y) = A^{(S)}(y)$ if and only if $y \notin S$. For $\varepsilon > 0$ and an oracle A from an oracle collection $\mathcal{A}$, let the *lower* (resp. *upper*) *ε-block sensitivity*, $\text{bs}^{\mathcal{A}}_{\varepsilon-}(f, A, |\phi\rangle)$ (resp. $\text{bs}^{\mathcal{A}}_{\varepsilon+}(f, A, |\phi\rangle)$), of f with an oracle A on an input $|\phi\rangle$ be the maximal integer ℓ such that there are ℓ nonempty, disjoint sets $\{S_i\}_{i=1}^{\ell}$ such that, for each $i \in [1,\ell]_{\mathbb{Z}}$, (i) $A^{(S_i)} \in \mathcal{A}$ and (ii) $f^{A^{(S_i)}}(|\phi\rangle) \leq f^A(|\phi\rangle) - \varepsilon$ (resp. $f^A(|\phi\rangle) \leq f^{A^{(S_i)}}(|\phi\rangle) + \varepsilon$).

First, we show an upper bound of $\text{bs}^{\mathcal{A}}_{\varepsilon-}(f, A, |\phi\rangle)$ and $\text{bs}^{\mathcal{A}}_{\varepsilon+}(f, A, |\phi\rangle)$. The notation $\eta^A_M(|\phi\rangle)$ denotes the acceptance probability of M with an oracle A on an input $|\phi\rangle$.

Proposition 17 *Let $\mathcal{A}$ be any set of oracles and let M be any well-formed oracle QTM whose running time $T(n)$ does not depend on the choice of oracles. Let $q\colon \mathbb{Z}^+ \to \mathbb{N}$ be a polynomially bounded function. For every x of length n, define $f^A(x) = \max\{\eta^A_M(|x\rangle \otimes |\phi\rangle)\}$ and $g^A(x) = \min\{\eta^A_M(|x\rangle \otimes |\phi\rangle)\}$, where the maximum and minimum are taken over all quantum pure states $|\phi\rangle$ of $q(n)$ qubits. Then, for any oracle $A \in \mathcal{A}$, any constant $\varepsilon > 0$, and any input x of length n,*

$$\begin{aligned} \text{bs}^{\mathcal{A}}_{\varepsilon-}(f, A, x) &\leq 4T(n)^2/\varepsilon^2, \\ \text{bs}^{\mathcal{A}}_{\varepsilon+}(g, A, x) &\leq 4T(n)^2/\varepsilon^2. \end{aligned}$$

For proving Proposition 17, we need two lemmas. The first lemma below is easy to show.

Lemma 18 *Let M and N be two well-formed QTMs. Let U_M and U_N be the unitary matrices for the time evolution of M and N, respectively. Then, $|\eta_M(|\phi\rangle) - \eta_N(|\psi\rangle)| \leq \|U_M|\phi\rangle - U_N|\psi\rangle\|$.*

The second lemma is a straightforward modification of Theorem 3.3 in [7]. Let $q^i_y(M, A, |\phi\rangle)$ denote the sum of the squared amplitudes associated with basis states with a string y in the query tape, for the superposition of all the configurations of M^A on input $|\phi\rangle$ at time i.

Lemma 19 *Let M be a well-formed oracle QTM whose running time $T(n)$ does not depend on the choice of oracles. For any oracles A and B, and for any two inputs $|\phi\rangle$ and $|\psi\rangle$ of n qubits,*

$$|\eta^A_M(|\phi\rangle) - \eta^B_M(|\psi\rangle)| \leq \||\phi\rangle - |\psi\rangle\| + 2\sqrt{T(n)} \left(\sum_{i=1}^{T(n)-1} \sum_{y \in A \triangle B} q^i_y(M, A, |\phi\rangle) \right)^{1/2}.$$

Proof. Let $|\phi_0\rangle = |\phi\rangle$ and $|\psi_0\rangle = |\psi\rangle$. For each $i \in [1, T(n)]_{\mathbb{Z}}$, let $|\phi_i\rangle = U_A|\phi_{i-1}\rangle$ and $|E_i\rangle = U_A|\phi_i\rangle - U_B|\phi_i\rangle$.

Note that $|\phi_{T(n)}\rangle = U_B^{T(n)}|\phi_0\rangle + \sum_{i=0}^{T(n)-1} U_B^{T(n)-i-1}|E_i\rangle$. Thus,

$$\begin{aligned}
\||\phi_{T(n)}\rangle - |\psi_{T(n)}\rangle\| &= \left\| U_B^{T(n)}(|\phi\rangle - |\psi\rangle) + \sum_{i=0}^{T(n)-1} U_B^{T(n)-i-1}|E_i\rangle \right\| \\
&\leq \|U_B^{T(n)}(|\phi\rangle - |\psi\rangle)\| + \sum_{i=0}^{T(n)-1} \|U_B^{T(n)-i-1}|E_i\rangle\| \\
&= \||\phi\rangle - |\psi\rangle\| + \sum_{i=0}^{T(n)-1} \||E_i\rangle\| \\
&\leq \||\phi\rangle - |\psi\rangle\| + \sqrt{T(n)} \left(\sum_{i=0}^{T(n)-1} \||E_i\rangle\|^2 \right)^{1/2},
\end{aligned}$$

where the last inequality comes from the Cauchy-Schwartz inequality. Since we consider only configurations of M in $|\phi_i\rangle$ which makes a query from $A \triangle B$, we have $\||E_i\rangle\|^2 \leq 4 \sum_{y \in A \triangle B} q_y^i(M, A, |\phi\rangle)$, and thus

$$\sum_{i=0}^{T(n)-1} \||E_i\rangle\|^2 \leq 4 \sum_{i=0}^{T(n)} \sum_{y \in A \triangle B} q_y^i(M, A, |\phi\rangle).$$

Now the lemma follows from Lemma 18, which ensures $|\eta_M^A(|\phi\rangle) - \eta_M^B(|\psi\rangle)| \leq \||\phi_{T(n)}\rangle - |\psi_{T(n)}\rangle\|$. □

Now we give the proof of Proposition 17.

Proof of Proposition 17. We show only the case of upper ε-block sensitivity. Let $l = \mathrm{bs}_{\varepsilon-}^{\mathcal{A}}(f, A, x)$, which is witnessed by nonempty, disjoint sets $\{S_j\}_{1 \leq j \leq l}$. Let $|\phi\rangle$ and $|\psi\rangle$ be quantum pure states of $q(n)$ qubits such that $f^A(x) = \eta_M^A(|x\rangle \otimes |\phi\rangle)$ and $f^{A^{(S_j)}}(x) = \eta_M^{A^{(S_j)}}(|x\rangle \otimes |\psi\rangle)$.

By the choice of S_j, we have

$$\eta_M^A(|x\rangle \otimes |\phi\rangle) - \eta_M^{A^{(S_j)}}(|x\rangle \otimes |\psi\rangle) \geq \varepsilon.$$

Note that $\eta_M^{A^{(S_j)}}(|x\rangle \otimes |\psi\rangle) \geq \eta_M^{A^{(S_j)}}(|x\rangle \otimes |\phi\rangle)$ because of the maximality of $|\psi\rangle$. Hence,

$$|\eta_M^A(|x\rangle \otimes |\phi\rangle) - \eta_M^{A^{(S_j)}}(|x\rangle \otimes |\phi\rangle)| \geq \varepsilon.$$

Since $A^{(S_j)} \triangle A = S_j$, by Lemma 19, we have, for each j,

$$\varepsilon^2 \leq 4T(n) \sum_{i=1}^{T(|x|)-1} \sum_{y \in S_j} q_y^i(M, A, |x\rangle \otimes |\phi\rangle).$$

Combining all j's, we have

$$\begin{aligned}
l\varepsilon^2 &\leq 4T(n) \sum_{j=1}^{l} \sum_{i=1}^{T(n)-1} \sum_{y \in S_j} q_y^i(M, A, |x\rangle \otimes |\phi\rangle) \\
&\leq 4T(n) \sum_{i=1}^{T(n)-1} \sum_{y \in \Sigma^*} q_y^i(M, A, |x\rangle \otimes |\phi\rangle) \leq 4T(n) \sum_{i=1}^{T(n)-1} \||\phi_i\rangle\|^2 \leq 4(T(n))^2.
\end{aligned}$$

Thus we have the assertion. □

Now, we are ready to show Theorem 15.

Proof of Theorem 15. Let $L^A = \{0^n \mid |A \cap \{0,1\}^n| = \emptyset\}$ for each $A \subseteq \{0,1\}^*$. Let $\mathcal{A} = \{A \mid \forall n[|A \cap \{0,1\}^n| \leq 1]\}$. Obviously, $L^A \in \text{co-UP}^A$ for any set A in $\mathcal{A}$, and thus $L^A \in \Pi_1^{\mathrm{P}}(A)$. We then show that $L^A \notin \mathrm{QMA}(k)^A$ for a certain set A in $\mathcal{A}$.

Let $\{M_i\}_{i \in \mathbb{Z}^+}$ be an effective enumeration of all QTMs running in polynomial time. The construction of A is done by stages. For the base case, let $A_0 = \emptyset$. In the nth stage for $n > 0$, $A_n \subseteq \{0,1\}^n$ is to be defined. Our desired A is defined as $A = \bigcup_i A_i$.

Now, consider the nth QTM M_n. Let $B = \cup_{i<n} A_i$. Note that $0^n \in L^B$. For simplicity, define $f^B(x) = \max\{\Pr_{M_n}[M_n(|x\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{k(|x|)}\rangle) = 1]\}$, where each $|\phi_i\rangle$, $1 \leq i \leq k(|x|)$, runs over all quantum pure states of $q(|x|)$ qubits for some fixed polynomial q.

Suppose $f^B(0^n) < 2/3$. Then we set A_n to be B and go to the next stage.

Now suppose $f^B(0^n) \geq 2/3$. Let $B_i = B \cup \{s_i^n\}$, where s_i^n is the ith element in $\{0,1\}^n$. Clearly, $0^n \notin L^{B_i}$ for all i's. We want to show that there exists a number i such that $f^{B_i}(0^n) > 1/3$. If so, force A_n to be such the B_i. Towards a contradiction, we assume that, for all i, $f^{B_i}(0^n) \leq 1/3$. By our assumption, $f^B(0^n) - f^{B_i}(0^n) \geq 1/3$ for all $i \in [1, 2^n]_{\mathbb{Z}}$. This implies that $\mathrm{bs}_{\frac{1}{3}-}^{2^{\Sigma^*}}(f, B, 0^n) \geq 2^n$, since $\{B_i\}_{i=1}^{2^n}$ is mutually disjoint. This contradicts Proposition 17. $\square$

7 Discussions

Here we show that there is no positive operator value measurement (POVM) that determines whether a given unknown state is in a tensor product form or even maximally entangled. Thus Arthur cannot rule out quantum proofs that are far from states of a tensor product of unentangled quantum states.

Suppose we have a quantum subroutine which 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 that consists of n qubits:

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

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

As for the proof $|\Psi\rangle$ which does not satisfy (a) nor (b), this subroutine may answer (a) or (b) at random. In the rest of this section, it is proved that this kind of subroutines cannot be realized by any physical method. In fact, we prove a stronger theorem which claims that the set of states in tensor product form cannot be distinguished even from the set of maximally entangled states by any physical operation. Here, the state $\rho = |\Psi\rangle\langle\Psi|$ is said to be *maximally entangled* if $|\Psi\rangle$ can be written by

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

where $d = 2^n$ is the dimension of $\mathcal{H}$ and each $\{|e_1\rangle, \ldots, |e_d\rangle\}$ and $\{|f_1\rangle, \ldots, |f_d\rangle\}$ is an orthonormal basis of $\mathcal{H}$ [8]. Among all states, maximally entangled states are farthest away from states in 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 20 *Suppose 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* $\mathsf{H}_0 = \{|\Psi_0\rangle\langle\Psi_0| \mid |\Psi_0\rangle \in \mathcal{H}^{\otimes 2},\ \exists|\psi\rangle, |\phi\rangle \in \mathcal{H},\ |\Psi_0\rangle = |\psi\rangle \otimes |\phi\rangle\}$,

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

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

Proof. Let $\boldsymbol{M} = \{M_0, M_1\}$ be a POVM on a given $|\Psi\rangle\langle\Psi|$. With $\boldsymbol{M}$ we conclude $|\Psi\rangle\langle\Psi| \in \mathsf{H}_i$ if $\boldsymbol{M}$ results in i, $i = 0, 1$. 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 which minimizes $\mathrm{P}^{\boldsymbol{M}}_{0\to 1}(|\Psi\rangle\langle\Psi|)$ keeping the other side of error small enough. More precisely, we want to evaluate $\mathcal{E}$ defined and bounded as follows.

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

where each μ_i is an arbitrary probability measure in H_i. This means 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 on the set $\{|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|\}_{i=1}^{d}{}_{j=1}^{d}$, that is, $\mu_0(|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|) = 1/d^2$ for each i, j, where $\{|e_1\rangle, \dots, |e_d\rangle\}$ is an orthonormal basis of $\mathcal{H}$, and take μ_1 as a uniform distribution on the set $\{|g_{m,n}\rangle\langle g_{m,n}|\}_{m=1}^{d}{}_{n=1}^{d}$, that is, $\mu_1(|g_{m,n}\rangle\langle g_{m,n}|) = 1/d^2$ for each m and n, where

$$|g_{m,n}\rangle = \frac{1}{d}\sum_{j=1}^{d} \left(e^{2\pi\sqrt{-1}jm/d} |e_j\rangle \otimes |e_{(j+n) \bmod d}\rangle \right).$$

This $\{|g_{1,1}\rangle, \dots, |g_{d,d}\rangle\}$ is an orthonormal basis of $\mathcal{H}^{\otimes 2}$ [9], and we have

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

Thus we have the assertion. □

From Theorem 20, it is easy to show the following corollary.

Corollary 21 *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* $\mathsf{H}_0 = \{|\Psi_0\rangle\langle\Psi_0| \mid |\Psi_0\rangle \in \mathcal{H}^{\otimes 2},\ \exists|\psi\rangle, |\phi\rangle \in \mathcal{H},\ |\Psi_0\rangle = |\psi\rangle \otimes |\phi\rangle\}$,

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

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

8 Conclusions

This paper pointed out that it is unclear whether the multi-proof model of quantum Merlin-Arthur proof systems collapses to the usual single-proof model. To investigate the possibility that quantum multi-proof systems collapse to quantum single-proof systems, this paper proved several basic properties such as a necessary and sufficient condition under which the number of quantum proofs is reducible to two. However, the central question whether multiple quantum proofs are really more helpful to Arthur still remains open. The authors hope that this paper sheds light on new features of quantum Merlin-Arthur proof systems and quantum complexity theory.

Acknowledgements

The authors are grateful of John H. Watrous for providing us with an unpublished proof of QMA $\subseteq$ PP, which was shown jointly by Alexei Yu. Kitaev and John H. Watrous. The first author thanks Richard E. Cleve and Lance J. Fortnow for their helpful comments.

References

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

[2] Dorit Aharonov, Alexei Yu. 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.

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

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

[5] 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.

[6] Robert M. Beals, Harry M. Buhrman, Richard E. Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *39th Annual Symposium on Foundations of Computer Science*, pages 352–361, 1998.

[7] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[8] 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.

[9] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard O. 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.

[10] Ethan Bernstein and Umesh V. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.
Preliminary version appeared in *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, pages 11–20, 1993.

[11] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani P. Roychowdhury, and Farrokh Vatan. A new universal and fault-tolerant quantum basis. *Information Processing Letters*, 75(3):101–107, 2000.
Preliminary version entitled "On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for Shor's basis" appeared in *40th Annual Symposium on Foundations of Computer Science*, pages 486–494, 1999.

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

[13] Ding-Zhu Du and Ker-I Ko. *Theory of Computational Complexity*. John Wiley & Sons, 2000.

[14] Stephen A. Fenner, Frederic Green, Steven Homer, and Randall Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proceedings of the Royal Society of London A*, 455:3953–3966, 1999.

[15] Lance J. Fortnow and John D. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.
Preliminary version appeared in *Proceedings, Thirteenth Annual IEEE Conference on Computational Complexity*, pages 202–209, 1998.

[16] Lance J. Fortnow, John Rompel, and Michael Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134(2):545–557, 1994.
Preliminary version appeared in *Proceedings, Structure in Complexity Theory, Third Annual Conference*, pages 156–161, 1988.

[17] Lance J. Fortnow and Michael Sipser. Are there interactive protocols for co-NP languages? *Information Processing Letters*, 28(5):249–251, 1988.

[18] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[19] Jozef D. Gruska. *Quantum Computing*. McGraw-Hill, 1999.

[20] Alexander S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*. North-Holland, 1982.

[21] Dominik Janzing, Pawel Wocjan, and Thomas Beth. Cooling and low energy state preparation for 3-local Hamiltonians are FQMA-complete. Los Alamos e-print archive, quant-ph/0303186, 2003.

[22] Dominik Janzing, Pawel Wocjan, and Thomas Beth. "Identity check" is QMA-complete. Los Alamos e-print archive, quant-ph/0305050, 2003.

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

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

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

[26] 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.

[27] Alexei Yu. Kitaev and John H. 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.

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

[29] 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.
Preliminary version appeared in *Algorithms and Computation, 13th International Symposium, ISAAC 2002*, volume 2518 of *Lecture Notes in Computer Science*, pages 115–127, 2002.

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

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

[32] Masanao Ozawa and Harumichi Nishimura. Local transition functions of quantum Turing machines. *Theoretical Informatics and Applications*, 34(5):379–402, 2000.

[33] Peter W. Shor. Fault-tolerant quantum computation. In *37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996.

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

[35] Pawel Wocjan and Thomas Beth. The 2-local Hamiltonian problem encompasses NP. Los Alamos e-print archive, quant-ph/0301087, 2003.

[36] Pawel Wocjan, Dominik Janzing, and Thomas Beth. Two QCMA-complete problems. Los Alamos e-print archive, quant-ph/0305090, 2003.

[37] Tomoyuki Yamakami. A foundation of programming a multi-tape quantum Turing machine. In *Mathematical Foundations of Computer Science 1999, 24th International Symposium, MFCS'99*, volume 1672 of *Lecture Notes in Computer Science*, pages 430–441, 1999.

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

[39] Andrew C.-C. Yao. Quantum circuit complexity. In *34th Annual Symposium on Foundations of Computer Science*, pages 352–361, 1993.