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

Hirotada Kobayashi[1,2], Keiji Matsumoto[3,1], and Tomoyuki Yamakami[4]

[1] 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
hirotada@qci.jst.go.jp
[2] Department of Information Science,
Graduate School of Science, The University of Tokyo,
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
[3] Foundations of Information Research Division, National Institute of Informatics,
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
keiji@nii.ac.jp
[4] School of Information Technology and Engineering, University of Ottawa,
800 King Edward Avenue, Ottawa, Ontario, Canada K1N 6N5
yamakami@site.uottawa.ca

Abstract. This paper introduces quantum "multiple-Merlin"-Arthur proof systems in which Arthur uses multiple quantum proofs unentangled with each other for his verification. Although classical multi-proof systems are obviously equivalent to classical single-proof systems, it is unclear whether quantum multi-proof systems collapse to quantum single-proof systems. This paper presents a necessary and sufficient condition under which the number of quantum proofs is reducible to two. It is also proved that using multiple quantum proofs does not increase the power of quantum Merlin-Arthur proof systems in the case of perfect soundness, and that 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 in which powerful Merlin, a prover, presents a proof and Arthur, a verifier, probabilistically verifies its correctness with high success probability. The resulting complexity class MA has played important roles in computational complexity theory [3,5,4].

A quantum analogue of MA was first discussed by Knill [15] and studied intensively by Kitaev [12], Watrous [17], and several very recent works such as [11, 2]. 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 with each other.

T. Ibaraki, N. Katoh, and H. Ono (Eds.): ISAAC 2003, LNCS 2906, pp. 189–198, 2003.

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 pure states might be advantageous to Arthur. 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 pure states, Arthur first runs some pre-processing to rule out any quantum proof far from states of a tensor product of two pure states, and then performs the verification procedure for two-proof systems. It turns out that this straightforward method does not work well, since there is no positive operator-valued measurement (POVM) that determines whether a given unknown state is in a tensor product form or even maximally entangled, as is shown in Section 6. 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 QMA $\subseteq$ PSPACE [12,13]) no longer works well for the multi-proof cases with a straightforward modification. Also, the existing proofs for the property that parallel repetition of a single-proof protocol reduces the error probability to be arbitrarily small [14,17,13] cannot be applied to the multi-proof cases.

For these reasons, this paper introduces the multi-proof model of quantum Merlin-Arthur proof systems. 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 that makes V 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 $b(n)$. The resulting complexity class is denoted by $\mathrm{QMA}(k, a, b)$. We often abbreviate $\mathrm{QMA}(k, 2/3, 1/3)$ as $\mathrm{QMA}(k)$ throughout this paper.

This paper presents a necessary and sufficient condition under which the number of quantum proofs is reducible to two. Our condition is related to the possibility of amplifying success probabilities without increasing the number of quantum proofs. More formally, $\mathrm{QMA}(k, a, b) = \mathrm{QMA}(2, 2/3, 1/3)$ for every constant $k \geq 2$ and any two-sided bounded error probability (a, b) if and only if $\mathrm{QMA}(k, a, b) = \mathrm{QMA}(k, 2/3, 1/3)$ for every constant $k \geq 2$ and any two-sided bounded error probability (a, b).

Our proof for this also implies an interesting consequence for the case of perfect completeness. Namely, $\mathrm{QMA}(k, 1, b) = \mathrm{QMA}(1, 1, 1/2)$ for every constant $k \geq 2$ and any bounded error probability b if and only if $\mathrm{QMA}(2, 1, b) = \mathrm{QMA}(1, 1, 1/2)$ for any bounded error probability b.

It is also proved for the case of perfect soundness that, for every k and any error probability a, $\mathrm{QMA}(k, a, 0) = \mathrm{QMA}(1, a, 0)$. With further analyses, the class NQP, which derives from another concept of "quantum nondeterminism" introduced by Adleman, DeMarrais, and Huang [1], 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 in which $\mathrm{QMA}(k)$ does not contain co-NP (actually co-UP) for every k. As an

immediate consequence, we have that, for every k, there exists a relativized world in which none of BQP, QMA(k), and co-QMA(k) coincides with each other.

Familiarity with the basics of quantum computation and information theory is assumed throughout this paper. The reader may refer to [10,16,13], for instance.

2 Quantum Merlin-Arthur Proof Systems

Here we formally define the multi-proof quantum Merlin-Arthur proof systems. 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, these two models of quantum Merlin-Arthur proof systems are clearly equivalent in view of computational power. Here we formalize both of these two types of models. In the subsequent sections we will choose a suitable model from them depending on the situations. Throughout this paper all input strings are over the alphabet $\Sigma = \{0, 1\}$, and $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of natural numbers and nonnegative integers, respectively.

A *quantum proof of size s* is a pure quantum state of s qubits. Given polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$, a *$(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V for k-proof quantum Merlin-Arthur proof systems* is a polynomial-time computable mapping of the form $V \colon \Sigma^* \to \Sigma^*$. For every input 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. V receives k quantum proofs $|\phi_1\rangle, \ldots, |\phi_k\rangle$, each of size $q_{\mathcal{M}}(n)$, and uses at most $q_{\mathcal{V}}(n)$ qubits for his private computation. 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 $|0^{q_{\mathcal{V}}(n)}\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_k\rangle$. Or in terms of quantum Turing machines, a $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V for k-proof quantum Merlin-Arthur proof systems is a multi-tape polynomial-time well-formed quantum Turing machine with two special tapes for an input and proofs other than the work tape. V receives k quantum proofs of size $q_{\mathcal{M}}(n)$ in the proof tape and uses at most $q_{\mathcal{V}}(n)$ cells in the work tape. The probability that V accepts the input is defined to be the probability that an observation of the output qubit (in the $\{|0\rangle, |1\rangle\}$ basis) yields $|1\rangle$, after V halts. More generally, the number of quantum proofs may not necessarily be a constant, and may be a function $k \colon \mathbb{Z}^+ \to \mathbb{N}$ of the input length n, but must be bounded polynomial in n.

Strictly speaking, the circuit-based $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier and the Turing-machine-based one may have different computational power for each fixed functions $q_{\mathcal{V}}$ and $q_{\mathcal{M}}$. They are, however, "polynomially equivalent" and make no difference in the definition of the class QMA(k, a, b) below.

Definition 1. *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* 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 for k-proof quantum Merlin-Arthur proof systems 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 $b(n)$.

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 abbreviate $\mathrm{QMA}(k, 2/3, 1/3)$ as $\mathrm{QMA}(k)$ for each k.

3 Condition under Which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$

Besides our central question whether quantum multi-proof Merlin-Arthur proof systems collapse to quantum single-proof systems, it is also unclear whether 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, here we give a condition under which $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ for every constant $k \geq 2$.

Formally, we consider the following condition on the possibility of amplifying success probabilities without increasing the number of quantum proofs:

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

Then we have the following theorem.

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

The proof of Theorem 2 uses the following key lemma, which is proved later.

Lemma 3. *For every $l \in \mathbb{N}$, every $r \in \{0, 1, 2\}$, and any two-sided bounded error probability (a, b) satisfying $a > 1 - (1-b)^2/10 \geq b$, $\mathrm{QMA}(3l + r, a, b) \subseteq \mathrm{QMA}\big(2l + r, a, 1 - (1-b)^2/10\big)$.*

Proof of Theorem 2. The "only if" part is obvious. We only show the "if" part.

Suppose that the condition $(*)$ holds. Then we have $\mathrm{QMA}(3l + r, a, b) = \mathrm{QMA}(3l + r, 99/100, 1/100)$ for every $l \in \mathbb{N}$, $r \in \{0, 1, 2\}$, and any two-sided bounded error probability (a, b). Now from Lemma 3, 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, $(*)$ ensures that $\mathrm{QMA}(2l + r, 99/100, 90199/100000) = \mathrm{QMA}(2l + r, 99/100, 1/100)$. Thus, we have $\mathrm{QMA}(3l + r, 99/100, 1/100) = \mathrm{QMA}(2l + r, 99/100, 1/100)$. We repeat this c times for some constant c of $O(\log_{3/2} k)$, and finally we obtain that $\mathrm{QMA}(3l + r, a, b) = \mathrm{QMA}(2, 99/100, 1/100)$. Again from $(*)$, $\mathrm{QMA}(2, 99/100, 1/100) = \mathrm{QMA}(2, a, b)$ for any two-sided bounded error probability (a, b). Therefore we have $\mathrm{QMA}(k, a, b) = \mathrm{QMA}(2, 2/3, 1/3)$ for every constant $k \geq 2$ and any two-sided bounded error probability (a, b). □

Now we give a proof of Lemma 3. The proof uses a special operator called *controlled-swap* that exchanges the contents of two registers $\mathbf{S}_1$ and $\mathbf{S}_2$ if control register $\mathbf{B}$ contains 1, and does nothing otherwise. Consider the *C-SWAP*

algorithm described below. A similar idea was used in [9] for the 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 H to $\mathbf{B}$. Accept if $\mathbf{B}$ contains 0, and otherwise reject.

We state the following without a proof, which is useful in proving Lemma 3.

Proposition 4. *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 of Lemma 3. The essence of the proof is the basis case where $k = 1$ and $r = 0$. We give the proof only for this particular case and leave the general case to the reader, since it is straightforward to modify our proof to the general case.

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

Let V be the quantum verifier of the original $(3, a, b)$-quantum Merlin-Arthur proof system. 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 $\big(2, a, 1 - (1-b)^2/10\big)$-quantum Merlin-Arthur proof system 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 $|D_1\rangle = |C_1\rangle \otimes |C_3\rangle$ and $|D_2\rangle = |C_2\rangle \otimes |C_3\rangle$, 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 $|D_1\rangle$ in registers $(\mathbf{R}_1, \mathbf{S}_1)$ and $|D_2\rangle$ 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 $\mathbf{B}$, $\mathbf{S}_1$, and $\mathbf{S}_2$.
     Accept if $\mathbf{B}$ contains 0, and 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 $\mathbf{V}$, $\mathbf{R}_1$, $\mathbf{R}_2$, and $\mathbf{S}_1$.
     Accept iff the result corresponds to the acceptance computation of the original quantum verifier.

The completeness of this protocol is immediate.

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 $\delta = (-1 + 2b + 4\sqrt{1 + b - b^2})/5$.

If $\mathrm{tr}(\rho\sigma) \leq \delta$, the probability α that the input x is accepted in the SEPARABILITY TEST is at most

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

Hence W accepts x with probability at most $(1+\alpha)/2 \leq 1 - (1-b)^2/10$.

On the other hand, if $\mathrm{tr}(\rho\sigma) > \delta$, 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 $F(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|) > \delta$. Therefore,

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

This implies that the input x is accepted in the CONSISTENCY TEST with probability at most $\beta < b + \sqrt{1-\delta^2}$, 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 $(1+\delta)/2 = b + \sqrt{1-\delta^2}$, one can see that $\beta < 1 - (1-b)^2/5$. Hence W accepts x with probability at most $(1+\beta)/2 < 1 - (1-b)^2/10$. □

4 One-Sided Bounded Error Cases

First we focus on the cases with perfect completeness. Together with the fact that parallel repetition works well for single-proof quantum Merlin-Arthur proof systems, Lemma 3 implies the following. The proof is easy and thus omitted.

Theorem 5. $\mathrm{QMA}(k,1,b) = \mathrm{QMA}(1,1,1/2)$ *for every constant* $k \geq 2$ *and any bounded error probability* b *if and only if* $\mathrm{QMA}(2,1,b) = \mathrm{QMA}(1,1,1/2)$ *for any bounded error probability* b.

Now we turn to the cases with perfect soundness. For such cases, multiple quantum proofs do not increase the computational power.

Theorem 6. *For any polynomially bounded function* $k\colon \mathbb{Z}^+ \to \mathbb{N}$ *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 $k(n)$ 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, the verifier W receives one quantum proof of size $k(n)q(n)$ and simulates V with this quantum proof.

The completeness property is clearly satisfied.

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 $k(n)q(n)$. Let e_i be the lexicographically ith string in $\{0,1\}^{k(n)q(n)}$. Note that, for each i, $1 \leq i \leq 2^{k(n)q(n)}$, V never accepts x when given $k(n)$ quantum proofs that form $|e_i\rangle$. Since any $|D\rangle$ is expressed as a linear combination of all $|e_i\rangle$, $1 \leq i \leq 2^{k(n)q(n)}$, 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. Theorem 6 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 7. *A language L is in* $\mathrm{NQMA}(k)$ *if there exists a function* $a\colon \mathbb{Z}^+ \to (0, 1]$ *such that L is in* $\mathrm{QMA}(k, a, 0)$.

$\mathrm{NQMA}(k) = \mathrm{NQMA}(1)$ is also immediate from Theorem 6. Actually, the following can be proved. This also gives a characterization of NQP by the union of $\mathrm{QMA}(1, a, 0)$ over all error probability functions a. The proof is omitted due to limitation of space.

Theorem 8. $\mathrm{EQMA}(1) \subseteq \mathrm{RQMA}(1) \subseteq \mathrm{NQMA}(1) = \mathrm{NQP}$.

5 Relativized Separation of QMA(k)

To see a limitation of $\mathrm{QMA}(k)$, here we show a relativized world in which $\mathrm{QMA}(k)$ does not contain co-UP.

Theorem 9. *For any polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$, there exists an oracle A relative to which* $\text{co-UP}^A \nsubseteq \mathrm{QMA}(k)^A$.

The following is an immediate corollary of Theorem 9.

Corollary 10. *For any polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$, there exists an oracle A relative to which none of* BQP, $\mathrm{QMA}(k)$, *and* co-$\mathrm{QMA}(k)$ *coincides with each other.*

Proof. By Theorem 9, we have an oracle A such that $\text{co-NP}^A \nsubseteq \mathrm{QMA}(k)^A$. Since $\text{co-NP}^A \subseteq \text{co-QMA}(k)^A$, it follows that $\text{co-QMA}(k)^A \nsubseteq \mathrm{QMA}(k)^A$, and thus $\mathrm{QMA}(k)^A \neq \text{co-QMA}(k)^A$. That $\mathrm{BQP}^A \neq \mathrm{QMA}(k)^A$ follows from $\mathrm{QMA}(k)^A \neq \text{co-QMA}(k)^A$. □

In what follows, we give the proof of Theorem 9. We use a so-called *block sensitivity* argument, whose quantum version was developed in [6]. Let $f\colon \Sigma^* \to [0, 1]$ be any relativizable function. 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* $\mathrm{bs}^{\mathcal{A}}_{\varepsilon-}(f, A, |\phi\rangle)$

(resp. $\mathrm{bs}^{\mathcal{A}}_{\varepsilon+}(f, A, |\phi\rangle)$) of f with an oracle A on an input $|\phi\rangle$ be the maximal integer l satisfying that there are l nonempty, disjoint sets $\{S_i\}_{i=1}^{l}$ such that, for every i, $1 \leq i \leq l$, (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 give an upper bound for each of $\mathrm{bs}^{\mathcal{A}}_{\varepsilon-}(f, A, |\phi\rangle)$ and $\mathrm{bs}^{\mathcal{A}}_{\varepsilon+}(f, A, |\phi\rangle)$. The notation $\eta^{A}_{M}(|\phi\rangle)$ denotes the acceptance probability of M with an oracle A on an input $|\phi\rangle$. The proof is omitted due to limitation of space.

Proposition 11. *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 pure states $|\phi\rangle$ of $q(n)$ qubits. Then, for every oracle $A \in \mathcal{A}$, every input x of length n, and any constant $\varepsilon > 0$, both of $\mathrm{bs}^{\mathcal{A}}_{\varepsilon-}(f, A, x)$ and $\mathrm{bs}^{\mathcal{A}}_{\varepsilon+}(g, A, x)$ are at most $4T(n)^2/\varepsilon^2$.*

Now we give a proof of Theorem 9.

Proof of Theorem 9. Let $L^{A} = \{0^j \mid |A \cap \{0,1\}^j| = \emptyset\}$ for each $A \subseteq \{0,1\}^*$. Let $\mathcal{A} = \{A \mid \forall j[|A \cap \{0,1\}^j| \leq 1]\}$. Obviously, $L^{A} \in \text{co-UP}^{A}$ for any set A in $\mathcal{A}$, and thus $L^{A} \in \Pi^{\mathrm{P}}_{1}(A)$. 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 jth stage for $j > 0$, $A_j \subseteq \{0,1\}^j$ is to be defined. Our desired A is defined as $A = \bigcup_i A_i$.

Now consider the jth QTM M_j. Let $B = \cup_{i<j} A_i$. Note that $0^j \in L^{B}$. For simplicity, define $f^{B}(x) = \max\{\Pr_{M_j}[M_j(|x\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{k(n)}\rangle) = 1]\}$ for every x of length n, where each $|\phi_i\rangle$, $1 \leq i \leq k(n)$, runs over all pure states of $q(n)$ qubits for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$.

Suppose that $f^{B}(0^j) < 2/3$. Then we set A_j to be B and go to the next stage.

Now suppose that $f^{B}(0^j) \geq 2/3$. Let $B_i = B \cup \{s^j_i\}$, where s^j_i is the ith element in $\{0,1\}^j$. Clearly, $0^j \notin L^{B_i}$ for all i's. We show that there exists a number i such that $f^{B_i}(0^j) > 1/3$. If so, force A_j to be such B_i. Towards a contradiction, we assume that, for all i, $f^{B_i}(0^j) \leq 1/3$. By our assumption, $f^{B}(0^j) - f^{B_i}(0^j) \geq 1/3$ for all i, $1 \leq i \leq 2^j$. It follows that $\mathrm{bs}^{2^{\Sigma^*}}_{\frac{1}{3}-}(f, B, 0^j) \geq 2^j$, since $\{B_i\}_{i=1}^{2^j}$ is mutually disjoint. This contradicts Proposition 11. □

6 Discussions

Here we show that there is no positive operator-valued measurement (POVM) that determines whether a given unknown state is in a tensor product form or even maximally entangled. Recall that the state $\rho = |\Psi\rangle\langle\Psi|$ is *maximally entangled* if $|\Psi\rangle$ can be written by $|\Psi\rangle = \sum_{i=1}^{d} \alpha_i |e_i\rangle \otimes |f_i\rangle$, $|\alpha_i|^2 = 1/d$, 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 $\mathcal{H}$ [7]. Among all states, maximally entangled states are farthest away from states in tensor product form, and

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

is achieved by maximally entangled states. Thus Arthur cannot rule out quantum proofs that are far from states of a tensor product of pure states.

Theorem 12. *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 POVM 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 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 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.

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

where each μ_i is an arbitrary probability measure in H_i. 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 such that $\mu_0(|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|) = 1/d^2$ for each i and j, where $\{|e_1\rangle, \ldots, |e_d\rangle\}$ is an orthonormal basis of $\mathcal{H}$, and μ_1 such that $\mu_1(|g_{m,n}\rangle\langle g_{m,n}|) = 1/d^2$ 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 $\{|g_{1,1}\rangle, \ldots, |g_{d,d}\rangle\}$ is an orthonormal basis of $\mathcal{H}^{\otimes 2}$ [8], and thus $\int_{\rho\in\mathsf{H}_0} \rho\mu_0(\mathrm{d}\rho) = \int_{\rho\in\mathsf{H}_1} \rho\mu_1(\mathrm{d}\rho) = I_{\mathcal{H}^{\otimes 2}}/d^2$. Hence we have the assertion. □

7 Conclusions

This paper pointed out that it is unclear whether the multi-proof model of quantum Merlin-Arthur proof systems collapses to the single-proof model and 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 to 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. L. M. Adleman, J. DeMarrais, and M.-D. A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.
2. D. Aharonov and O. Regev. A lattice problem in quantum NP. In *44th Annual Symposium on Foundations of Computer Science*, 2003. To appear.
3. L. Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.
4. L. Babai. Bounded round interactive proofs in finite groups. *SIAM Journal on Discrete Mathematics*, 5(1):88–111, 1992.
5. L. Babai and S. 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. R. M. Beals, H. M. Buhrman, R. E. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *39th Annual Symposium on Foundations of Computer Science*, pages 352–361, 1998.
7. C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046–2052, 1996.
8. C. H. Bennett, G. Brassard, C. Crépeau, R. O. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.
9. H. M. Buhrman, R. E. Cleve, J. H. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.
10. J. D. Gruska. *Quantum Computing*. McGraw-Hill, 1999.
11. J. Kempe and O. Regev. 3-local Hamiltonian is QMA-complete. *Quantum Information and Computation*, 3(3):258–264, 2003.
12. A. Yu. Kitaev. Quantum NP. Talk at the 2nd Workshop on Algorithms in Quantum Information Processing, DePaul University, Chicago, January 1999.
13. A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.
14. A. Yu. Kitaev and J. 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.
15. E. H. Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996.
16. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
17. J. H. Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual Symposium on Foundations of Computer Science*, pages 537–546, 2000.