EXP Upper Bound for Multi-Proof QMA of Perfect Completeness

Hirotada Kobayashi[1*] Keiji Matsumoto[12†]

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

Abstract. Kobayashi, Matsumoto, and Yamakami posed a question whether quantum "multiple-Merlin"-Arthur proof systems in which Arthur uses multiple quantum proofs unentangled with each other for his verification are computationally equivalent to the usual quantum Merlin-Arthur proof systems with a single quantum proof. In particular, they pointed out that the existing proofs for QMA $\subseteq$ PP and even for QMA $\subseteq$ PSPACE no longer work well in the case of quantum multi-proof systems, and only the trivial upper bound of NEXP is known for them. This paper gives the first non-trivial upper bound of EXP for quantum multi-proof systems of perfect completeness.

Keywords: quantum complexity theory, quantum Merlin-Arthur proof systems

1 Introduction

Babai [1] introduced Merlin-Arthur proof systems in which powerful Merlin as a prover presents a proof and Arthur as 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 [1, 3, 2].

A quantum analogue of MA was first discussed by Knill [6] and studied intensively by Kitaev [4], Watrous [8], and a number of very recent works. 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. Kobayashi, Matsumoto, and Yamakami [7] introduced the model in which Arthur receives *multiple* quantum proofs unentangled with each other, and posed a question whether this model is computationally equivalent to the usual single-proof model of quantum Merlin-Arthur proof systems.

One of the properties that hold for the single-proof case but are not known to hold for the multi-proof cases is on the upper bound of the power of quantum Merlin-Arthur proof systems. Namely, the unpublished proof by Kitaev and Watrous for the upper bound PP of the class QMA of languages having single-proof quantum Merlin-Arthur proof systems (and even the proof of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 [4, 5]) no longer works well for the multi-proof cases with a straightforward modification. Only the trivial upper bound of NEXP is known for the multi-proof cases.

This paper gives the first non-trivial upper bound of EXP for quantum multi-proof systems of perfect completeness. Our proof involves a natural promise problem called the *Purity Preservable Quantum Channel* problem informally described as follows: given a quantum channel, is there any pure state as an input such that the channel outputs a pure state of a certain restricted form, or for any input pure state the channel outputs a state far from the desired form? More formally, our problem is parameterized by α and β such that the one with parameters $\alpha = 1$ and $\beta = b$ is complete for the class $\mathrm{QMA}(2,1,b)$ of problems having two-proof quantum Merlin-Arthur proof systems of perfect completeness with error probability $b < 1$ in soundness. It is proved that this promise problem with parameters $\alpha = 1$ and $\beta = b$ can be solved in deterministic exponential time for every nonnegative constant $b < 1$. For the case of perfect completeness, Kobayashi, Matsumoto, and Yamakami [7] implicitly proved that, for every constant $k \geq 2$ and every nonnegative constant $b_1 < 1$, the class $\mathrm{QMA}(k,1,b_1)$ of problems having k-proof quantum Merlin-Arthur proof systems of perfect completeness with error probability b_1 in soundness is necessarily contained in $\mathrm{QMA}(2,1,b_2)$ for some constant error probability $b_2 < 1$. Therefore, our claim essentially proves $\mathrm{QMA}(k,1,b) \subseteq \mathrm{EXP}$ for every constant k and every nonnegative constant $b < 1$ (actually it is provable for any error probability function b such that $1/(1-b(n))$ is bounded exponential in n).

2 Purity Preservable Quantum Channel

A q_{in}-*in* q_{out}-*out quantum channel* is a quantum circuit Q over q qubits that acts on a quantum state (not necessarily a pure state) of $q_{\mathrm{in}} \leq q$ qubits together with ancillae of $|0^{q-q_{\mathrm{in}}}\rangle$ and outputs a quantum state (again not neces-

*hirotada@qci.jst.go.jp
†keiji@nii.ac.jp

sarily a pure state) of q_{out} qubits. Our complete promise problem for $\mathrm{QMA}(2,a,b)$ is described as follows.

(α,β)-Purity Preservable Quantum Channel

Input: A description of a quantum channel Q of q_{in}-in q_{out}-out and an integer $r \leq q_{\text{out}}$.

Promise: One of the following two holds:

(a) there exists a pair of pure states $|\phi\rangle$ of q_{in} qubits and $|\psi\rangle$ of $q_{\text{out}}-r$ qubits such that an output quantum state ρ of Q with an input $|\phi\rangle$ satisfies $F(\rho,|\psi\rangle\langle\psi|\otimes|0^r\rangle\langle 0^r|) \geq \alpha$,

(b) for any pair of pure states $|\phi\rangle$ of q_{in} qubits and $|\psi\rangle$ of $q_{\text{out}}-r$ qubits, an output quantum state ρ of Q with an input $|\phi\rangle$ satisfies $F(\rho,|\psi\rangle\langle\psi|\otimes|0^r\rangle\langle 0^r|) \leq \beta$.

Output: Accept if (a) is satisfied, and otherwise reject.

That the (a,b)-Purity Preservable Quantum Channel is in $\mathrm{QMA}(2,a,b)$ is rather trivial. To see the hardness, notice that the accepting probability of the verifier V in a two-proof QMA protocol is given by $\max_{|\phi\rangle,|\psi\rangle,|\psi'\rangle} |\langle 1|\langle\phi|V|0^{q_{\mathcal{V}}}\rangle|\psi\rangle|\psi'\rangle|^2$. Identifying Q with $V^{\dagger}$, this is equal to $\max_{|\phi\rangle,|\psi\rangle} F(\rho,|\psi\rangle\langle\psi|\otimes|0^{q_{\mathcal{V}}}\rangle\langle 0^{q_{\mathcal{V}}}|)$, and the completeness follows.

Theorem 1 *For every constants a,b satisfying $0 \leq b < a \leq 1$, (a,b)-Purity Preservable Quantum Channel is complete for* $\mathrm{QMA}(2,a,b)$.

3 QMA(k, 1, b) $\subseteq$ EXP

It is proved that there is a deterministic exponential-time algorithm for the (α,β)-Purity Preservable Quantum Channel problem with parameters $\alpha = 1$ and $\beta = b$. As an immediate corollary, we have the EXP upper bound for the class $\mathrm{QMA}(2,1,b)$.

Theorem 2 *For every nonnegative constant $\beta < 1$, there is a deterministic exponential-time algorithm that solves $(1,\beta)$-Purity Preservable Quantum Channel.*

Corollary 3 *For every nonnegative constant $b < 1$,* $\mathrm{QMA}(2,1,b) \subseteq \mathrm{EXP}$.

For the k-proof QMA of perfect completeness, Kobayashi, Matsumoto, and Yamakami [7] implicitly proved that, for every constant $k \geq 2$ and every nonnegative constant $b_1 < 1$, $\mathrm{QMA}(k,1,b_1) \subseteq \mathrm{QMA}(2,1,b_2)$ for some nonnegative constant $b_2 < 1$. Hence we have the following theorem.

Theorem 4 *For every $k \in \mathbb{N}$ and every nonnegative constant $b < 1$,* $\mathrm{QMA}(k,1,b) \subseteq \mathrm{EXP}$.

More generally, our proof is extendable to show the EXP upper bound for $\mathrm{QMA}(k,1,b)$ for any error probability function b such that $1/(1-b(n))$ is bounded exponential in n.

Theorem 5 *For every $k \in \mathbb{N}$ and any function $b\colon \mathbb{Z}^+ \to [0,1]$ satisfying $b(n) < 1 - 1/\mu(n)$ for some exponentially bounded function $\mu\colon \mathbb{Z}^+ \to \mathbb{N}$,* $\mathrm{QMA}(k,1,b) \subseteq \mathrm{EXP}$.

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.

References

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

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

[3] 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.

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

[5] 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.

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

[7] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, *Lecture Notes in Computer Science*, 2003. To appear.

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