Quantum Verifiers with Multiple Quantum Certificates

Hirotada Kobayashi[*†] hirotada@is.s.u-tokyo.ac.jp

Keiji Matsumoto[†] keiji@qci.jst.go.jp

Tomoyuki Yamakami[‡] yamakami@site.uottawa.ca

The class MA is a randomized generalization of the class NP. A quantum analogue of MA was apparently first discussed by Knill, was later studied by Kitaev, and was named QMA by Watrous. Intuitively, MA (QMA) is the class of languages that can be efficiently verified by classical (quantum) verifiers using single classical (quantum) certificate. Consider a situation that a verifier receives not only one but multiple certificates. In the classical setting, it is obvious that a classical verifier with multiple classical certificates is essentially the same to that with single classical certificate. However, in the quantum setting where a quantum verifier is given a set of quantum certificates in the tensor product form, the situation seems to be different, because the quantum verifier might utilize the structure of the tensor product form. From this point of view, we extend the definition of QMA to QMA(k) for the case quantum verifiers use k quantum certificates.

Formally, we define quantum verifiers in terms of quantum circuits. For each input $x \in \Sigma^*$, of length $n = |x|$, each quantum certificate $|C_i\rangle$ is a quantum pure state consists of $q_{\mathcal{M}}(n)$ qubits. Besides $kq_{\mathcal{M}}(n)$ qubits for the certificates, we have $q_{\mathcal{V}}(n)$ qubits called *private qubits* in our quantum circuit. 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 any 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 $|0^{q_{\mathcal{V}}(n)}\rangle \otimes |C_1\rangle \otimes \cdots \otimes |C_k\rangle$.

Definition 1 *For a positive integer k and functions $a, b \colon \mathbb{Z}^+ \to [0,1]$, a language L is in $QMA(k,a,b)$ if there exist polynomial 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 any x of length n,*

(i) if $x \in L$, there exists a set of quantum certificates $|C_1\rangle, \dots, |C_k\rangle$ of $q_{\mathcal{M}}(n)$ qubits which causes V accept x with probability at least $a(n)$,

(ii) if $x \notin L$, given any sets of quantum certificates $|C'_1\rangle, \dots, |C'_k\rangle$ of $q_{\mathcal{M}}(n)$ qubits, V accepts x with probability at most $b(n)$.

Based on this model, we show that any one-sided bounded error protocol with a quantum verifier using k quantum certificates can be simulated by a protocol with a quantum verifier using only two quantum certificates with one-sided bounded error for any positive integer $k \geq 2$. For this, we first show the following theorem:

Theorem 2 *For any fixed positive integer k and any $r \in \{0,1,2\}$ and any polynomial bounded function $p \colon \mathbb{Z}^+ \to \mathbb{R}^+, p \geq 1$,*

$$QMA(3k+r, 1, 1-1/p) \subseteq QMA\big(2k+r, 1, 1-1/(10p^2)\big).$$

Applying this theorem repeatedly, we obtain the following theorem:

Theorem 3 *For any fixed positive integer k and any polynomial bounded function $p_1 \colon \mathbb{Z}^+ \to \mathbb{R}^+, p_1 \geq 1$, there exists a polynomial bounded function $p_2 \colon \mathbb{Z}^+ \to \mathbb{R}^+, p_2 \geq 1$ such that*

$$QMA(k, 1, 1-1/p_1) \subseteq QMA(2, 1, 1-1/p_2).$$

We do not know whether the parallel repetition of the protocol of polynomially many times reduces the error probability to be exponentially small.

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

[†]Quantum Computation and Information Project, ERATO, Japan Science and Technology Corporation, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

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