Quantum Multi-Prover Interactive Proof Systems with Limited Prior Entanglement

Hirotada Kobayashi[*†]
hirotada@qci.jst.go.jp

Keiji Matsumoto[‡*]
keiji@nii.ac.jp

[*]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

6 June 2003

Abstract

This paper gives the first formal treatment of a quantum analogue of multi-prover interactive proof systems. It is proved that the class of languages having quantum multi-prover interactive proof systems is necessarily contained in NEXP, under the assumption that provers are allowed to share at most polynomially many prior-entangled qubits. This implies that, in particular, if provers do not share any prior entanglement with each other, the class of languages having quantum multi-prover interactive proof systems is equal to NEXP. Related to these, it is shown that, in the case a prover does not have his private qubits, the class of languages having quantum single-prover interactive proof systems is also equal to NEXP.

1 Introduction

After Deutsch [13] gave the first formal treatment of quantum computation, a number of papers have provided evidence that quantum computation has much more power than classical computation for solving certain computational tasks, including notable Shor's integer factoring algorithm [33]. Watrous [35] showed that it might be also the case for single-prover interactive proof systems, by constructing a constant-round quantum interactive protocol for a PSPACE-complete language, which is impossible for classical interactive proof systems unless the polynomial-time hierarchy collapses to AM [4, 19]. A natural question to ask is how strong a quantum analogue of multi-prover interactive proof systems is. This paper gives the first step for this question, by proving that the class of languages having quantum multi-prover interactive proof systems is necessarily contained in non-deterministic

exponential time (NEXP), under the assumption that provers are allowed to share at most polynomially many prior-entangled qubits. This might even suggest that, under such an assumption, quantum multi-prover interactive proof systems are weaker than classical ones, since Cleve [12] reported that a pair of provers sharing polynomially many entangled qubits can in some sense cheat a classical verifier.

Interactive proof systems were introduced by Babai [4] and Goldwasser, Micali, and Rackoff [18]. An interactive proof system consists of an interaction between a computationally unbounded prover and a polynomial-time probabilistic verifier. The prover attempts to convince the verifier that a given input string satisfies some property, while the verifier tries to verify the validity of the assertion of the prover. A language L is said to have an interactive proof system if there exists a verifier V such that (i) in the case the input is in L, there exists a prover P that can convince V with certainty, and (ii) in the case the input is not in L, no prover P' can convince V with probability more than $1/2$. It is well-known that the class of languages having interactive proof systems, denoted by IP, is equal to PSPACE, shown by Shamir [30] based on the work of Lund, Fortnow, Karloff, and Nisan [26], and on the result of Papadimitriou [29] (see also [31]).

Quantum interactive proof systems were introduced by Watrous [35] in terms of quantum circuits. He showed that every language in PSPACE has a quantum interactive protocol, with exponentially small one-sided error, in which the prover and the verifier exchange only three messages. A consecutive work of Kitaev and Watrous [23] showed that any quantum interactive protocol, even with two-sided bounded error, can be parallelized to a three-message quantum protocol with exponentially small one-sided error. They also showed that the class of languages having quantum interactive proof systems is necessarily contained in deterministic exponential time (EXP).

A multi-prover interactive proof system, introduced by Ben-Or, Goldwasser, Kilian, and Wigderson [7], is an extension of a (single-prover) interactive proof system in which a verifier communicates with not only one but multiple provers, while provers cannot communicate with each other prover and cannot know messages exchanged between the verifier and other provers. A language L is said to have a multi-prover interactive proof system if, for some k denoting the number of provers, there exists a verifier V such that (i) in the case the input is in L, there exist provers $P_1, \ldots, P_k$ that can convince V with certainty, and (ii) in the case the input is not in L, no set of provers $P'_1, \ldots, P'_k$ can convince V with probability more than $1/2$. Babai, Fortnow, and Lund [5], combining the result by Fortnow, Rompel, and Sipser [17], showed that the class of languages having multi-prover interactive proof systems, denoted by MIP, is equal to NEXP. A sequence of papers by Cai, Condon, and Lipton [10, 11], Feige [14], and Lapidot and Shamir [25] led to a result of Feige and Lovász [15] that every language in NEXP has a two-prover interactive proof system with just one round (i.e. two messages) of communication (meaning that the verifier sends one question to each of the provers in parallel, then receives their responses), with exponentially small one-sided error.

In this paper we first define quantum multi-prover interactive proof systems by naturally extending the quantum single-prover model. Perhaps the most important and interesting difference between quantum and classical multi-prover interactive proofs is that provers may share entanglement *a priori*. Particular cases are protocols with two provers initially sharing lots of EPR pairs. For the sake of generality, we may allow protocols with any number of provers and with any kind of prior entanglement, not limited to EPR-type ones. Although sharing classical randomness among provers does not change the power of classical multi-prover interactive proofs (unless zero-knowledge properties are taken into account [6]), sharing prior entanglement does have a possibility both to strengthen and to weaken the power of quantum multi-prover interactive proofs. In fact, while sharing prior entanglement may increase the power of cheating provers as shown by Cleve [12], it may be possible for a quantum verifier to turn the prior entanglement among provers to his advantage.

The main result of this paper is to show the NEXP upper bound for quantum multi-prover interactive proof systems under the assumption that provers are allowed to share at most polynomially many prior-entangled qubits. That is, polynomially many prior-entangled qubits among provers cannot be advantageous to a quantum verifier. As a special case of this result, it is proved that, if provers do

not share any prior entanglement with each other, the class of languages having quantum multi-prover interactive proof systems is equal to NEXP. Another result related to these is that, in the case the prover does not have his private qubits, the class of languages having quantum single-prover interactive proof systems is also equal to NEXP. This special model of quantum single-prover interactive proofs can be regarded as a quantum counterpart of a probabilistic oracle machine [17, 16, 5] in the sense that there is no private space for the prover during the protocol, and thus we call this model as a *quantum oracle circuit*. Our result shows that quantumization of probabilistic oracle machines does not change the power of the model.

To prove the NEXP upper bound of quantum multi-prover interactive proof systems, a key idea is to bound the number of private qubits of provers without diminishing the computational power of them. Suppose that each prover has only polynomially many private qubits during the protocol. Then the total number of qubits of the quantum multi-prover interactive proof system is polynomially bounded, and we can show that it can be simulated classically in non-deterministic exponential time. Now the point is whether space-bounded quantum provers (i.e. provers can apply any unitary transformations on their spaces, but the number of qubits in their spaces is bounded polynomial with respect to the input length) are as powerful as space-unbounded quantum provers or not. Under the assumption that provers are allowed to share at most polynomially many prior-entangled qubits, we show that, even with only polynomially many private qubits, each prover can do everything that he could with as many qubits as he likes, in the sense that the verifier cannot distinguish the difference at all. For this, we also prove one fundamental property on quantum information theory using the entanglement measure introduced by Nielsen [27]. Apart from quantum interactive proof systems, this property itself is also of interest and worth while stating.

The remainder of this paper is organized as follows. In Section 2 we briefly review basic notations and definitions in quantum computation and quantum information theory. In Section 3 we give a formal definition of quantum multi-prover interactive proof systems and quantum oracle circuits. In Section 4 we show our main result of the NEXP upper bound of quantum multi-prover interactive proof systems. In Section 5 we focus on the prior unentangled cases and on quantum oracle circuits. Finally we conclude with Section 6, which summarizes our results and mentions a number of open problems related to our work.

2 Quantum Fundamentals

Here we briefly review basic notations and definitions in quantum computation and quantum information theory. Detailed descriptions are, for instance, in [20, 28, 22].

A *pure state* is described by a unit vector in some Hilbert space. In particular, an n-dimensional pure state is a unit vector $|\psi\rangle$ in $\mathbb{C}^n$. Let $\{|e_1\rangle, \ldots, |e_n\rangle\}$ be an orthonormal basis for $\mathbb{C}^n$. Then any pure state in $\mathbb{C}^n$ can be described as $\sum_{i=1}^n \alpha_i |e_i\rangle$ for some $\alpha_1, \ldots, \alpha_n \in \mathbb{C}, \sum_{i=1}^n |\alpha_i|^2 = 1$.

A *mixed state* is a classical probability distribution $(p_i, |\psi_i\rangle)$, $0 \leq p_i \leq 1$, $\sum_i p_i = 1$ over pure states $|\psi_i\rangle$. This can be interpreted as being in the pure state $|\psi_i\rangle$ with probability p_i. A mixed state 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.

If a unitary transformation U is applied to a state $|\psi\rangle$, the state becomes $U|\psi\rangle$. In the form of density matrices, a state ρ changes to $U\rho U^\dagger$ after U is applied.

One of the important operations to density matrices is the *trace-out* operation. Given a density matrix ρ over $\mathcal{H} \otimes \mathcal{K}$, the state after tracing out $\mathcal{K}$ is a density matrix over $\mathcal{H}$ described by

$$\mathrm{tr}_{\mathcal{K}} \rho = \sum_{i=1}^{n} (I_{\mathcal{H}} \otimes \langle e_i|) \rho (I_{\mathcal{H}} \otimes |e_i\rangle)$$

for any orthonormal basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$ of $\mathcal{K}$, where n is the dimension of $\mathcal{K}$ and $I_{\mathcal{H}}$ is the identity

operator over $\mathcal{H}$. To perform this operation on some part of a quantum system gives a partial view of the quantum system with respect to the remaining part.

One of the important concepts in quantum physics is a *measurement*. Any collection of linear operators $\{A_1, \ldots, A_k\}$ satisfying $\sum_{i=1}^{k} A_i^\dagger A_i = I$ defines a measurement. If a system is in a pure state $|\psi\rangle$, such a measurement results in i with probability $\|A_i|\psi\rangle\|^2$, and the state becomes $A_i|\psi\rangle/\|A_i|\psi\rangle\|$. If a system is in a mixed state with a density matrix ρ, the result i is observed with probability $\mathrm{tr}(A_i \rho A_i^\dagger)$, and the state after the measurement is with a density matrix $A_i \rho A_i^\dagger / \mathrm{tr}(A_i \rho A_i^\dagger)$. A special class of measurements are *projection* or *von Neumann* measurements in which $\{A_1, \ldots, A_k\}$ is a collection of orthonormal projections. In this scheme, an observable is a decomposition of $\mathcal{H}$ into orthogonal subspaces $\mathcal{H}_1, \ldots, \mathcal{H}_k$, that is, $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_k$. It is important to note that two mixed states having the identical density matrix cannot be distinguished at all by any measurement.

For any linear operator A over $\mathcal{H}$, the l_2-norm of A is defined by

$$\|A\| = \sup_{|\psi\rangle \in \mathcal{H} \setminus \{0\}} \frac{\|A|\psi\rangle\|}{\||\psi\rangle\|}.$$

3 Definitions

3.1 Polynomial-Time Uniformly Generated Families of Quantum Circuits

Similar to the model of quantum single-prover interactive proof systems discussed in [35, 23], we define quantum multi-prover interactive proof systems in terms of quantum circuits. Before proceeding to the definition of quantum multi-prover interactive proof systems, we review the concept of polynomial-time uniformly generated families of quantum circuits.

A family $\{Q_x\}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a deterministic procedure that, on every input x, outputs a description of Q_x and runs in time polynomial in $n = |x|$. For simplicity, we assume all input strings are over the alphabet $\Sigma = \{0, 1\}$. It is assumed that the circuits in such a family are composed of gates in some reasonable, universal, finite set of quantum gates such as the Shor basis [32, 9]: Hadamard gates, $\sqrt{\sigma_z}$ gates, and Toffoli gates. Furthermore, it is assumed that the number of gates in any circuit is not more than the length of the description of that circuit. Therefore Q_x must have size polynomial in n. For convenience, we may identify a circuit Q_x with the unitary operator it induces.

It should be mentioned that to permit non-unitary quantum circuits, in particular, to permit measurements at any timing during the computation does not change the computational power of the model in view of time complexity. See [1] for a detailed description of the equivalence of the unitary and non-unitary quantum circuit models.

3.2 Quantum Multi-Prover Interactive Proof Systems

Here we give a formal definition of quantum multi-prover interactive proof systems which is a natural extension of quantum single-prover ones defined by Watrous [35]. In fact, the model of quantum single-prover interactive proof systems discussed in [35, 23] is a special case of our quantum multi-prover model with the restriction of the number of provers to one.

Let k be the number of provers. For every input $x \in \Sigma^*$ of length $n = |x|$, the entire system of quantum k-prover interactive proof system consists of $q(n) = q_{\mathcal{V}}(n) + \sum_{i=1}^{k} (q_{\mathcal{M}_i}(n) + q_{\mathcal{P}_i}(n))$ qubits, where $q_{\mathcal{V}}(n)$ is the number of qubits that are private to a verifier V, each $q_{\mathcal{P}_i}(n)$ is the number of qubits that are private to a prover P_i, and each $q_{\mathcal{M}_i}(n)$ is the number of message qubits used for communication between V and P_i. Note that no communication is allowed between different provers P_i and P_j. It is assumed that $q_{\mathcal{V}}$ and each $q_{\mathcal{M}_i}$ are polynomially bounded functions. Moreover, without loss of generality, we may assume that $q_{\mathcal{M}_1} = \cdots = q_{\mathcal{M}_k} = q_{\mathcal{M}}$ and $q_{\mathcal{P}_1} = \cdots = q_{\mathcal{P}_k} = q_{\mathcal{P}}$. Accordingly, the entire system consists of $q(n) = q_{\mathcal{V}}(n) + k(q_{\mathcal{M}}(n) + q_{\mathcal{P}}(n))$ qubits.

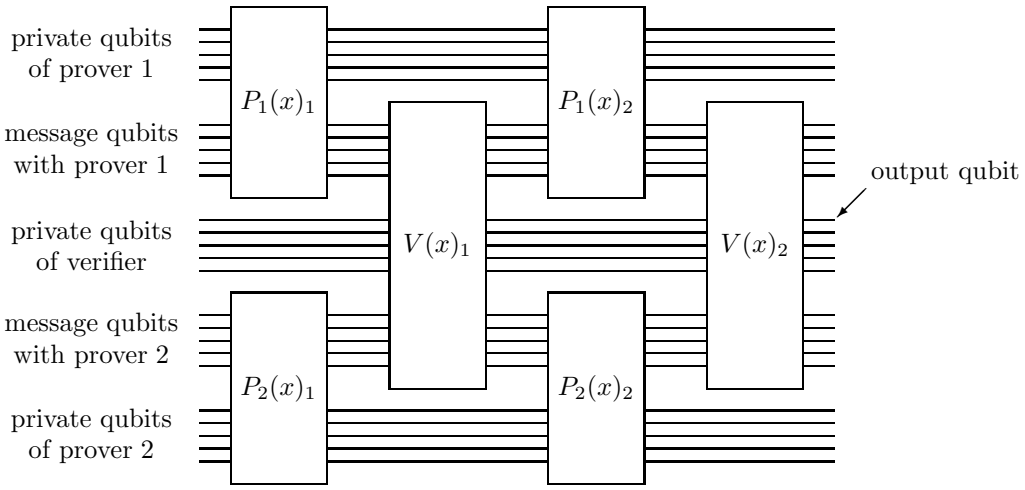

Figure 1: Quantum circuit for a three-message quantum two-prover interactive proof system

Given polynomially bounded functions $m, q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$, an *$m$-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier* V for a quantum k-prover interactive proof system is a polynomial-time computable mapping of the form $V \colon \Sigma^* \to \Sigma^*$, where $\Sigma = \{0,1\}$ is the alphabet set. For every input $x \in \Sigma^*$ of length n, V uses at most $q_{\mathcal{V}}(n)$ qubits for his private space and at most $q_{\mathcal{M}}(n)$ qubits for communication with each prover. The string $V(x)$ is interpreted as a $\lfloor m(n)/2+1 \rfloor$-tuple $(V(x)_1, \ldots, V(x)_{\lfloor m(n)/2+1 \rfloor})$, with each $V(x)_j$ a description of a polynomial-time uniformly generated quantum circuit acting on $q_{\mathcal{V}}(n) + kq_{\mathcal{M}}(n)$ qubits. One of the private qubits of the verifier is designated as the output qubit.

Given polynomially bounded functions $m, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and a function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$, an *$m$-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover* P_i for each $i = 1, \ldots, k$ is a mapping of the form $P_i \colon \Sigma^* \to \Sigma^*$. For every input $x \in \Sigma^*$ of length n, each P_i uses at most $q_{\mathcal{P}}(n)$ qubits for his private space and at most $q_{\mathcal{M}}(n)$ qubits for communication with the verifier. The string $P_i(x)$ is interpreted as a $\lfloor m(n)/2+1/2 \rfloor$-tuple $(P_i(x)_1, \ldots, P_i(x)_{\lfloor m(n)/2+1/2 \rfloor})$, with each $P_i(x)_j$ a description of a quantum circuit acting on $q_{\mathcal{M}}(n) + q_{\mathcal{P}}(n)$ qubits. No restrictions are placed on the complexity of the mapping P_i (i.e., each $P_i(x)_j$ can be an arbitrary unitary transformation). Furthermore, for some function $q_{\mathrm{ent}} \colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $q_{\mathrm{ent}} \leq q_{\mathcal{P}}$, each P_i may have at most $q_{\mathrm{ent}}(n)$ qubits among his private qubits that are prior-entangled with some private qubits of other provers. Such a prover P_i is said *q_{ent}-prior-entangled*. For the sake of generality, we allow any kind of prior entanglement, not limited to EPR-type ones.

An *m-message $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum k-prover interactive proof system* consists of an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V and m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum provers $P_1, \ldots, P_k$. If $P_1, \ldots, P_k$ are q_{ent}-prior-entangled, such a quantum k-prover interactive proof system is said *q_{ent}-prior-entangled*. Let $\mathcal{V} = l_2(\Sigma^{q_{\mathcal{V}}})$, each $\mathcal{M}_i = l_2(\Sigma^{q_{\mathcal{M}}})$, and each $\mathcal{P}_i = l_2(\Sigma^{q_{\mathcal{P}}})$ denote the Hilbert spaces corresponding to the private qubits of the verifier, the message qubits between the verifier and the ith prover, and the private qubits of the ith prover, respectively. Given a verifier V, provers $P_1, \ldots, P_k$, and an input x of length n, we define a circuit $(P_1(x), \ldots, P_k(x), V(x))$ acting on $q(n)$ qubits as follows. If $m(n)$ is odd, circuits $P_1(x)_1, \ldots, P_k(x)_1$, $V(x)_1$, …, $P_1(x)_{(m(n)+1)/2}, \ldots, P_k(x)_{(m(n)+1)/2}$, $V(x)_{(m(n)+1)/2}$ are applied in sequence, each $P_i(x)_j$ to $\mathcal{M}_i \otimes \mathcal{P}_i$, and each $V(x)_j$ to $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k$. If $m(n)$ is even, circuits $V(x)_1$, $P_1(x)_1, \ldots, P_k(x)_1$, …, $V(x)_{m(n)/2}$, $P_1(x)_{m(n)/2}, \ldots, P_k(x)_{m(n)/2}$, $V(x)_{m(n)/2+1}$ are applied in sequence. Figure 1 illustrates the situation for the case $k = 2$ and $m(n) = 3$. Note that the order of applications of the circuits of the provers at each round has actually no sense since the space $\mathcal{M}_i \otimes \mathcal{P}_i$ on which the circuits of the ith prover act is separated from each other prover.

At any given instant, the state of the entire system is a unit vector in the space $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes$

$\mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$. For instance, in the case $m(n) = 3$, given an input x of length n, the state of the system after all of the circuits of the provers and the verifier have been applied is

$$V_2 P_{k,2} \cdots P_{1,2} V_1 P_{k,1} \cdots P_{1,1} |\psi_{\text{init}}\rangle,$$

where each V_j and $P_{i,j}$ denotes the extension of $V(x)_j$ and $P_i(x)_j$, respectively, to the space $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$ by tensoring with the identity, and $|\psi_{\text{init}}\rangle \in \mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$ denotes the initial state. In the initial state $|\psi_{\text{init}}\rangle$ for q_{ent}-prior-entangled proof systems, only the first $q_{\text{ent}}(n)$ qubits in each $\mathcal{P}_i$ may be entangled with other qubits in $\mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$. All the qubits other than these prior-entangled ones are initially in the $|0\rangle$-state.

For every input x, the probability that the $(k+1)$-tuple $(P_1, \ldots, P_k, V)$ accepts x is defined to be the probability that an observation of the output qubit in the basis of $\{|0\rangle, |1\rangle\}$ yields $|1\rangle$, after the circuit $(P_1(x), \ldots, P_k(x), V(x))$ is applied to the initial state $|\psi_{\text{init}}\rangle$.

Although k, the number of provers, has been treated to be constant so far, the above definition can be naturally extended to the case that $k\colon \mathbb{Z}^+ \to \mathbb{N}$ is a function of the input length n. In what follows, we treat k as a function. Note that the number of provers possible to communicate with the verifier must be bounded polynomial in n.

Definition 1 *Given polynomially bounded functions $k, m\colon \mathbb{Z}^+ \to \mathbb{N}$, a function $q_{\text{ent}}\colon \mathbb{Z}^+ \to \mathbb{N}$, and functions $a, b\colon \mathbb{Z}^+ \to [0,1]$, a language L is in* $\mathrm{QMIP}(k, m, q_{\text{ent}}, a, b)$ *iff there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V for a quantum k-prover interactive proof system such that, for every input x of length n,*

(i) if $x \in L$, there exist a function $q_{\mathcal{P}}\colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $q_{\mathcal{P}} \geq q_{\text{ent}}$ and a set of k quantum provers $P_1, \ldots, P_k$ of m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted q_{ent}-prior-entangled such that $(P_1, \ldots, P_k, V)$ accepts x with probability at least $a(n)$,

(ii) if $x \notin L$, for all functions $q'_{\mathcal{P}}\colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $q'_{\mathcal{P}} \geq q_{\text{ent}}$ and all sets of k quantum provers $P'_1, \ldots, P'_k$ of m-message $(q_{\mathcal{M}}, q'_{\mathcal{P}})$-restricted q_{ent}-prior-entangled, $(P'_1, \ldots, P'_k, V)$ accepts x with probability at most $b(n)$.

Let $\mathrm{QMIP}(poly, poly, q_{\text{ent}}, a, b)$ denote the union of the classes $\mathrm{QMIP}(k, m, q_{\text{ent}}, a, b)$ over all polynomially bounded functions k and m. The class QMIP of languages having quantum multi-prover interactive proof systems is defined as follows.

Definition 2 *A language L is in* QMIP *iff there exists a function $q_{\text{ent}}\colon \mathbb{Z}^+ \to \mathbb{N}$ such that, for any function $q'_{\text{ent}}\colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $q'_{\text{ent}} \geq q_{\text{ent}}$, L is in* $\mathrm{QMIP}(poly, poly, q'_{\text{ent}}, 1, 1/2)$.

Next we define the class $\mathrm{QMIP}^{(\text{l.e.})}$ of languages having quantum multi-prover interactive proof systems with at most polynomially many prior-entangled qubits.

Definition 3 *A language L is in* $\mathrm{QMIP}^{(\text{l.e.})}$ *iff there exists a polynomially bounded function $q_{\text{ent}}\colon \mathbb{Z}^+ \to \mathbb{N}$ such that, for any polynomially bounded function $q'_{\text{ent}}\colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $q'_{\text{ent}} \geq q_{\text{ent}}$, L is in* $\mathrm{QMIP}(poly, poly, q'_{\text{ent}}, 1, 1/2)$.

Finally we define the class $\mathrm{QMIP}^{(\text{n.e.})}$ of languages having quantum multi-prover interactive proof systems without any prior entanglement.

Definition 4 *A language L is in* $\mathrm{QMIP}^{(\text{n.e.})}$ *iff L is in* $\mathrm{QMIP}(poly, poly, 0, 1, 1/2)$.

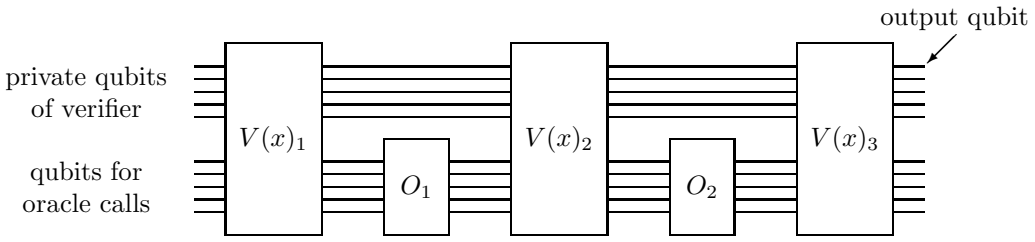

Figure 2: Quantum circuit for a two-oracle-call quantum oracle circuit

3.3 Quantum Oracle Circuits

Consider a situation in which a verifier can communicate with only one prover, but the prover does not have his private qubits. We call this model a *quantum oracle circuit*, since it can be regarded as a quantum counterpart of a probabilistic oracle machine [17, 16, 5] in the sense that there is no private space for the prover during the protocol.

For the definition of quantum oracle circuits, we use slightly different terminologies from those in the previous subsection so that they are fitted to the term 'oracle' rather than 'prover'.

Given polynomially bounded functions $m, q_{\mathcal{V}}, q_{\mathcal{O}} \colon \mathbb{Z}^+ \to \mathbb{N}$, an *$m$-oracle-call $(q_{\mathcal{V}}, q_{\mathcal{O}})$-restricted quantum verifier* V for a quantum oracle circuit is a $2m$-message $(q_{\mathcal{V}}, q_{\mathcal{O}})$-restricted quantum verifier for a quantum single-prover interactive proof system. A *$q_{\mathcal{O}}$-restricted quantum oracle* O for an m-oracle-call $(q_{\mathcal{V}}, q_{\mathcal{O}})$-restricted quantum verifier is a $2m$-message $(q_{\mathcal{O}}, 0)$-restricted quantum prover. Figure 2 illustrates the situation of a two-oracle-call quantum oracle circuit. Note that our definition of a quantum oracle completely differs from the one by Bennett, Bernstein, Brassard, and Vazirani [8] in which a quantum oracle is restricted to a unitary transformation that maps $|y, z\rangle$ to $|y, z \oplus f(y)\rangle$ in one step for an arbitrary function $f \colon \{0,1\}^* \to \{0,1\}$.

Definition 5 *Given a polynomially bounded function $m \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $a, b \colon \mathbb{Z}^+ \to [0,1]$, a language L is in* $\mathrm{QOC}(m, a, b)$ *iff there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{O}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and an m-oracle-call $(q_{\mathcal{V}}, q_{\mathcal{O}})$-restricted quantum verifier V for a quantum oracle circuit such that, for every input x of length n,*

(i) if $x \in L$, there exists a $q_{\mathcal{O}}$-restricted quantum oracle O for V such that V with access to O accepts x with probability at least $a(n)$,

(ii) if $x \notin L$, for all $q_{\mathcal{O}}$-restricted quantum oracles O' for V, V with access to O' accepts x with probability at most $b(n)$.

Let $\mathrm{QOC}(poly, a, b)$ denote the union of the classes $\mathrm{QOC}(m, a, b)$ over all polynomially bounded functions m. The class QOC of languages accepted by quantum oracle circuits is defined as follows.

Definition 6 *A language L is in* QOC *iff L is in* $\mathrm{QOC}(poly, 1, 1/2)$.

4 $\mathbf{QMIP}^{(\mathrm{l.e.})} \subseteq \mathbf{NEXP}$

Now we show that every language having a quantum multi-prover interactive proof system is necessarily in NEXP under the assumption that provers are allowed to share at most polynomially many prior-entangled qubits.

A key idea of our proof is to bound the number of private qubits of provers without diminishing the computational power of them. First, in Subsection 4.1, we explain our bounding technique with the

single-prover case, which is much easier to understand. Although our result for the single-prover case only gives the NEXP upper bound for the class QIP of quantum single-prover interactive proofs, it will be much of help to understand our key idea of the proof for the multi-prover case in Subsection 4.2. For simplicity, in this section and after, we often drop the argument x and n in the various functions defined in the previous section. We also assume that operators acting on subsystems of a given system are extended to the entire system by tensoring with the identity, when it is clear from context upon what part of a system a given operator acts.

4.1 Single-Prover Case

First we show that, for any protocol of quantum single-prover interactive proof systems, there exists a quantum single-prover interactive protocol exchanging the same number of messages, in which the prover uses only polynomially many qubits for his private space with respect to input length, and the probability of acceptance is exactly equal to that of the original one. To show this, the following two theorems play very important roles. A point of our proof is how to combine and apply these two to the theory of quantum interactive proof systems.

Theorem 7 ([34, 21]) *Let $|\phi\rangle, |\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ satisfy $\mathrm{tr}_{\mathcal{H}_2}|\phi\rangle\langle\phi| = \mathrm{tr}_{\mathcal{H}_2}|\psi\rangle\langle\psi|$. Then there is a unitary transformation U over $\mathcal{H}_2$ such that $(I_{\mathcal{H}_1} \otimes U)|\phi\rangle = |\psi\rangle$, where $I_{\mathcal{H}_1}$ is the identity operator over $\mathcal{H}_1$.*

Theorem 8 ([28], page 110) *Let ρ be a density matrix over $\mathcal{H}_1$. Then there exist a Hilbert space $\mathcal{H}_2$ of $\dim(\mathcal{H}_2) = \dim(\mathcal{H}_1)$ and a pure state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ such that $\mathrm{tr}_{\mathcal{H}_2}|\psi\rangle\langle\psi| = \rho$.*

Now we give a proof of our claim.

Lemma 9 *Let $m, q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ be polynomially bounded functions and V be an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier for a quantum single-prover interactive proof system. Then, for any function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and any m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P, there exists an m-message $(q_{\mathcal{M}}, q_{\mathcal{V}} + q_{\mathcal{M}})$-restricted quantum prover P' such that, for every input x, the probability of accepting x by (P', V) is exactly equal to the one by (P, V).*

Proof. It is assumed that $q_{\mathcal{P}} \geq q_{\mathcal{V}} + q_{\mathcal{M}}$, since there is nothing to show in the case $q_{\mathcal{P}} < q_{\mathcal{V}} + q_{\mathcal{M}}$. It is also assumed that the values of m are even (odd cases can be dealt with a similar argument).

Given a protocol (P, V) of an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum single-prover interactive proof system, we construct an m-message $(q_{\mathcal{M}}, q_{\mathcal{V}} + q_{\mathcal{M}})$-restricted quantum prover P' such that the probability of acceptance by (P', V) is exactly equal to the one by (P, V) on every input. We construct P' by showing, for every input x, how to construct each $P'_j(x)$ based on the original $P_j(x)$. In the following proof, each $P_j(x)$ and $P'_j(x)$ will be abbreviated as P_j and P'_j, respectively.

Let $\mathcal{P}' = l_2(\Sigma^{q_{\mathcal{M}}+q_{\mathcal{V}}})$ be the Hilbert space corresponding to the private qubits of P'. Let each $|\psi_j\rangle, |\phi_j\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$, for $1 \leq j \leq m/2$, denote a state of the original m-message $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum interactive proof system defined in a recursive manner by

$$\begin{array}{lcll} |\phi_1\rangle & = & V_1|\psi_{\mathrm{init}}\rangle, & \\ |\phi_j\rangle & = & V_j P_{j-1}|\phi_{j-1}\rangle, & 2 \leq j \leq m/2, \\ |\psi_j\rangle & = & P_j|\phi_j\rangle, & 1 \leq j \leq m/2. \end{array}$$

Here $|\psi_{\mathrm{init}}\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ is the initial state in which all the qubits are the $|0\rangle$-states. Notice that $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}|\psi_j\rangle\langle\psi_j| = \mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}|\phi_j\rangle\langle\phi_j|$ for each $1 \leq j \leq m/2$, since each P_j acts only on the qubits in $\mathcal{M}\otimes\mathcal{P}$.

From Theorem 8, there exist states $|\psi'_j\rangle, |\phi'_j\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}'$ such that

$$\begin{array}{rcl} \mathrm{tr}_{\mathcal{P}'}|\phi'_j\rangle\langle\phi'_j| & = & \mathrm{tr}_{\mathcal{P}}|\phi_j\rangle\langle\phi_j|, \\ \mathrm{tr}_{\mathcal{P}'}|\psi'_j\rangle\langle\psi'_j| & = & \mathrm{tr}_{\mathcal{P}}|\psi_j\rangle\langle\psi_j|, \end{array}$$

for each $1 \leq j \leq m/2$. Thus we have

$$\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}'}|\psi'_j\rangle\langle\psi'_j| = \mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}|\psi_j\rangle\langle\psi_j| = \mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}|\phi_j\rangle\langle\phi_j| = \mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}'}|\phi'_j\rangle\langle\phi'_j|,$$

for each $1 \leq j \leq m/2$.

Therefore, by Theorem 7, there exists a unitary transformation P'_j acting on $\mathcal{M}\otimes\mathcal{P}'$ such that $P'_j|\phi'_j\rangle = |\psi'_j\rangle$ for each $1 \leq j \leq m/2$.

Having defined P'_j, $|\phi'_j\rangle$, and $|\psi'_j\rangle$ for each $1 \leq j \leq m/2$, compare the state just before the final measurement is performed in the original protocol and that in the constructed protocol. Let $|\phi_{m/2+1}\rangle = V_{m/2+1}|\psi_{m/2}\rangle$ and $|\phi'_{m/2+1}\rangle = V_{m/2+1}|\psi'_{m/2}\rangle$. These $|\phi_{m/2+1}\rangle$ and $|\phi'_{m/2+1}\rangle$ are exactly the states we want to compare. Noticing that $\mathrm{tr}_{\mathcal{P}}|\psi_{m/2}\rangle\langle\psi_{m/2}| = \mathrm{tr}_{\mathcal{P}'}|\psi'_{m/2}\rangle\langle\psi'_{m/2}|$, we have $\mathrm{tr}_{\mathcal{P}}|\phi_{m/2+1}\rangle\langle\phi_{m/2+1}| = \mathrm{tr}_{\mathcal{P}}|\phi'_{m/2+1}\rangle\langle\phi'_{m/2+1}|$, since $V_{m/2+1}$ acts only on $\mathcal{V}\otimes\mathcal{M}$. This implies that the verifier V cannot distinguish $|\phi'_{m/2+1}\rangle$ from $|\phi_{m/2+1}\rangle$ at all. Hence, for every input x, the probability of accepting x in the protocol (P', V) is exactly equal to the one in the original protocol (P, V). Thus we have the assertion. □

4.2 QMIP$^{(\mathrm{l.e.})} \subseteq$ NEXP

In the proof of Lemma 9 we decomposed the Hilbert space of the proof system into $\mathcal{V}\otimes\mathcal{M}$ and $\mathcal{P}$ and used Theorem 8 by taking $\mathcal{V}\otimes\mathcal{M}$ as a Hilbert space $\mathcal{H}_1$ of Theorem 8. For k-prover cases, however, if we focus on one fixed prover P_i and decompose the Hilbert space of the proof system into the private space of P_i and the rest, Theorem 8 is of no help, because the number of qubits of the proof system out of $\mathcal{P}_i$ may be no longer bounded polynomial in input length. Instead of Theorem 8, we show the following theorem, which is useful even for k-prover cases.

Theorem 10 *Fix a state $|\phi\rangle$ in $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3$ and a unitary transformation U over $\mathcal{H}_2\otimes\mathcal{H}_3$ arbitrarily, and let $|\psi\rangle$ denote $(I_{\mathcal{H}_1}\otimes U)|\phi\rangle$. Then, for any Hilbert space $\mathcal{H}'_3$ of $\dim(\mathcal{H}'_3) \leq \dim(\mathcal{H}_3)$ such that there is a state $|\phi'\rangle$ in $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}'_3$ satisfying $\mathrm{tr}_{\mathcal{H}'_3}|\phi'\rangle\langle\phi'| = \mathrm{tr}_{\mathcal{H}_3}|\phi\rangle\langle\phi|$, there exist a Hilbert space $\mathcal{H}''_3$ of $\dim(\mathcal{H}''_3) = (\dim(\mathcal{H}_2))^2\cdot\dim(\mathcal{H}'_3)$ and a state $|\psi'\rangle$ in $\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}''_3$ such that $\mathrm{tr}_{\mathcal{H}''_3}|\psi'\rangle\langle\psi'| = \mathrm{tr}_{\mathcal{H}_3}|\psi\rangle\langle\psi|$.*

For the proof of Theorem 10, we use the entanglement measure introduced by Nielsen [27]. Let us decompose a vector $|\xi\rangle \in \mathcal{H}_1\otimes\mathcal{H}_2$ into

$$|\xi\rangle = \sum_{i,j}\alpha_{ij}|e^1_i\rangle\otimes|e^2_j\rangle, \tag{1}$$

where $\{|e^1_i\rangle\}$ and $\{|e^2_i\rangle\}$ are orthonormal bases of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then the *entanglement measure* $\mathrm{ent}_2(|\xi\rangle, \mathcal{H}_1, \mathcal{H}_2)$ is defined by the minimum number of non-zero terms in the right hand side of (1), where the minimum is taken over all the possible choices of the bases $\{|e^1_i\rangle\}$ and $\{|e^2_i\rangle\}$. The decomposition with the minimum number of non-zero terms is given by the Schmidt decomposition [34],

$$|\xi\rangle = \sum_i \beta_i|e^1_i\rangle\otimes|e^2_i\rangle,$$

where each $|e^1_i\rangle$ and $|e^2_i\rangle$ is a normalized eigenvector of $\mathrm{tr}_{\mathcal{H}_1}|\xi\rangle\langle\xi|$ and $\mathrm{tr}_{\mathcal{H}_2}|\xi\rangle\langle\xi|$, respectively. Therefore, the entanglement measure $\mathrm{ent}_2(|\xi\rangle, \mathcal{H}_1, \mathcal{H}_2)$ is nothing but the minimum dimension of the Hilbert space $\mathcal{H}'_2$ such that there is a vector $|\xi'\rangle \in \mathcal{H}_1\otimes\mathcal{H}'_2$ that satisfies $\mathrm{tr}_{\mathcal{H}_2}|\xi\rangle\langle\xi| = \mathrm{tr}_{\mathcal{H}'_2}|\xi'\rangle\langle\xi'|$.

We extend the definition of $\mathrm{ent}_2(\cdot,\cdot,\cdot)$ to a three-party case. For a vector $|\zeta\rangle \in \mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3$, define the *three-party entanglement measure* $\mathrm{ent}_3(|\zeta\rangle, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3)$ as the minimum number of non-zero terms in the decomposition

$$|\zeta\rangle = \sum_{i,j,k}\gamma_{ijk}|e^1_i\rangle\otimes|e^2_j\rangle\otimes|e^3_k\rangle,$$

where $\{|e_i^j\rangle\}$ denotes an orthonormal basis of the space $\mathcal{H}_j$ for each $j = 1, 2, 3$.

Proof of Theorem 10. Since $\mathrm{ent}_2(|\psi\rangle, \mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_3)$ gives the minimum dimension of $\mathcal{H}_3''$ such that there is a state $|\psi'\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3''$ satisfying $\mathrm{tr}_{\mathcal{H}_3''}|\psi'\rangle\langle\psi'| = \mathrm{tr}_{\mathcal{H}_3}|\psi\rangle\langle\psi|$, it is sufficient to show that $\mathrm{ent}_2(|\psi\rangle, \mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_3) \leq \dim(\mathcal{H}_3') \cdot (\dim(\mathcal{H}_2))^2$. This can be proved as follows:

$$\begin{aligned}
\mathrm{ent}_2(|\psi\rangle, \mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_3) &\leq \mathrm{ent}_3(|\psi\rangle, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3) \\
&\leq \mathrm{ent}_3(|\phi\rangle, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3) \cdot \dim(\mathcal{H}_2) \\
&\leq \mathrm{ent}_2(|\phi\rangle, \mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_3) \cdot (\dim(\mathcal{H}_2))^2 \\
&\leq \dim(\mathcal{H}_3') \cdot (\dim(\mathcal{H}_2))^2.
\end{aligned}$$

The first inequality directly comes from the definition of the entanglement measure. To prove the second and third inequalities, let $|\phi\rangle = \sum_{i,j,k} \gamma_{ijk}|e_i^1\rangle \otimes |e_j^2\rangle \otimes |e_k^3\rangle$ be the decomposition of $|\phi\rangle$ with respect to the orthonormal bases $\{|e_i^1\rangle\}$, $\{|e_i^2\rangle\}$, and $\{|e_i^3\rangle\}$ of $\mathcal{H}_1$, $\mathcal{H}_2$, and $\mathcal{H}_3$, respectively, and let $|\phi\rangle = \sum_i \beta_i |f_i^{1,2}\rangle \otimes |f_i^3\rangle$ be that of $|\phi\rangle$ with respect to the orthonormal bases $\{|f_i^{1,2}\rangle\}$ and $\{|f_i^3\rangle\}$ of $\mathcal{H}_1 \otimes \mathcal{H}_2$ and $\mathcal{H}_3$, respectively. The second and third inequalities are the consequences of the equality

$$|\psi\rangle = \sum_{i,j,k} \gamma_{ijk}|e_i^1\rangle \otimes U(|e_j^2\rangle \otimes |e_k^3\rangle) = \sum_{i,j,k} \gamma_{ijk}|e_i^1\rangle \otimes \left(\sum_{l=1}^{\dim(\mathcal{H}_2)} \beta'_{jkl}|e_{jkl}^2\rangle \otimes |e_{jkl}^3\rangle \right)$$

and the equality

$$|\phi\rangle = \sum_i \beta_i |f_i^{1,2}\rangle \otimes |f_i^3\rangle = \sum_i \beta_i \left(\sum_{j=1}^{\dim(\mathcal{H}_2)} \beta''_{ij}|f_{ij}^1\rangle \otimes |f_{ij}^2\rangle \right) \otimes |f_j^3\rangle,$$

respectively, where $\sum_{l=1}^{\dim(\mathcal{H}_2)} \beta'_{jkl}|e_{jkl}^2\rangle \otimes |e_{jkl}^3\rangle$ and $\sum_{j=1}^{\dim(\mathcal{H}_2)} \beta''_{ij}|f_{ij}^1\rangle \otimes |f_{ij}^2\rangle$ are the Schmidt decompositions of $U(|e_j^2\rangle \otimes |e_k^3\rangle)$ and $|f_i^{1,2}\rangle$, respectively. The fourth inequality is from the definition of the entanglement measure, which ensures that $\mathrm{ent}_2(|\phi\rangle, \mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_3) \leq \dim(\mathcal{H}_3')$ holds. □

Now we are ready to show the following lemma.

Lemma 11 *Let $k, m, q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathrm{ent}} \colon \mathbb{Z}^+ \to \mathbb{N}$ be polynomially bounded functions and V be an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier for a quantum k-prover interactive proof system. Then, for any function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $q_{\mathcal{P}} \geq q_{\mathrm{ent}}$ and any set of m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted q_{ent}-prior-entangled quantum provers $P_1, \ldots, P_k$, there exists a set of m-message $(q_{\mathcal{M}}, q_{\mathrm{ent}} + 2\lfloor m/2 + 1/2 \rfloor q_{\mathcal{M}})$-restricted q_{ent}-prior-entangled quantum provers $P_1', \ldots, P_k'$ such that, for every input x, the probability of accepting x by $(P_1', \ldots, P_k', V)$ is exactly equal to the one by $(P_1, \ldots, P_k, V)$.*

Proof. It is assumed that $q_{\mathcal{P}} \geq q_{\mathrm{ent}} + 2\lfloor m/2 + 1/2 \rfloor q_{\mathcal{M}}$, since there is nothing to show in the case $q_{\mathcal{P}} < q_{\mathrm{ent}} + 2\lfloor m/2 + 1/2 \rfloor q_{\mathcal{M}}$. It is also assumed that the values of m are even, and thus $2\lfloor m/2 + 1/2 \rfloor q_{\mathcal{M}} = m q_{\mathcal{M}}$ (odd cases can be dealt with a similar argument).

Given a protocol $(P_1, \ldots, P_k, V)$ of an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted q_{ent}-prior-entangled quantum k-prover interactive proof system, we first show that P_1 can be replaced by an m-message $(q_{\mathcal{M}}, q_{\mathrm{ent}} + m q_{\mathcal{M}})$-restricted q_{ent}-prior-entangled quantum prover P_1' such that the probability of acceptance by $(P_1', P_2, \ldots, P_k, V)$ is exactly equal to the one by $(P_1, \ldots, P_k, V)$ on every input. Having shown this, we repeat the same process for each of provers to construct a protocol $(P_1', P_2', P_3, \ldots, P_k, V)$ from $(P_1', P_2, P_3, \ldots, P_k, V)$ and so on, and finally we obtain a protocol $(P_1', \ldots, P_k', V)$ in which all of $P_1', \ldots, P_k'$ are m-message $(q_{\mathcal{M}}, q_{\mathrm{ent}} + m q_{\mathcal{M}})$-restricted q_{ent}-prior-entangled quantum provers. We construct P_1' by showing, for every input x, how to construct each $P_{1,j}'(x)$ based on the original $P_{1,j}(x)$. In the following proof, each $P_{i,j}(x)$ and $P_{i,j}'(x)$ will be abbreviated as $P_{i,j}$ and $P_{i,j}'$, respectively.

Let each $|\psi_j\rangle, |\phi_j\rangle \in \mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$, for $1 \leq j \leq m/2$, denote a state of the original m-message $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted $q_{\rm ent}$-prior-entangled quantum k-prover interactive proof system defined in a recursive manner by

$$\begin{array}{rcll} |\phi_1\rangle & = & V_1|\psi_{\rm init}\rangle, & \\ |\phi_j\rangle & = & V_j P_{k,j-1} \cdots P_{1,j-1}|\phi_{j-1}\rangle, & 2 \leq j \leq m/2, \\ |\psi_j\rangle & = & P_{1,j}|\phi_j\rangle, & 1 \leq j \leq m/2. \end{array}$$

Here $|\psi_{\rm init}\rangle \in \mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$ is the initial state in which the first $q_{\rm ent}(n)$ qubits in each $\mathcal{P}_j$ may be entangled with private qubits of other provers than P_j. All the qubits other than these prior-entangled qubits are the $|0\rangle$-states in the state $|\psi_{\rm init}\rangle$. Note that $\mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\psi_j\rangle\langle\psi_j| = \mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\phi_j\rangle\langle\phi_j|$, for each $1 \leq j \leq m/2$.

We define each $P'_{1,j}$ recursively. To define $P'_{1,1}$, consider the states $|\phi_1\rangle$ and $|\psi_1\rangle$. Let $|\phi'_1\rangle = |\phi_1\rangle$. Since all of the last $(q_{\mathcal{P}} - q_{\rm ent})$ qubits in $\mathcal{P}_1$ in the state $|\phi_1\rangle$ are the $|0\rangle$-states and $|\psi_1\rangle = P_{1,1}|\phi_1\rangle$, by Theorem 10, there exists a state $|\psi'_1\rangle$ in $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$ such that

$$\mathrm{tr}_{\mathcal{P}_1}|\psi'_1\rangle\langle\psi'_1| = \mathrm{tr}_{\mathcal{P}_1}|\psi_1\rangle\langle\psi_1|$$

and all but the first $q_{\rm ent} + 2q_{\mathcal{M}}$ qubits in $\mathcal{P}_1$ are the $|0\rangle$-states in the state $|\psi'_1\rangle$. Furthermore we have

$$\mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\psi'_1\rangle\langle\psi'_1| = \mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\psi_1\rangle\langle\psi_1| = \mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\phi_1\rangle\langle\phi_1| = \mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\phi'_1\rangle\langle\phi'_1|.$$

Therefore, by Theorem 7, there exists a unitary transformation $Q_{1,1}$ acting on $\mathcal{M}_1 \otimes \mathcal{P}_1$ such that $Q_{1,1}|\phi'_1\rangle = |\psi'_1\rangle$ and $Q_{1,1}$ is of the form $P'_{1,1} \otimes I_{q_{\mathcal{P}} - q_{\rm ent} - mq_{\mathcal{M}}}$, where $P'_{1,1}$ is a unitary transformation acting on qubits in $\mathcal{M}_1$ and the first $q_{\rm ent} + mq_{\mathcal{M}}$ qubits of $\mathcal{P}_1$, and $I_{q_{\mathcal{P}} - q_{\rm ent} - mq_{\mathcal{M}}}$ is the $(q_{\mathcal{P}} - q_{\rm ent} - mq_{\mathcal{M}})$-dimensional identity matrix.

Assume that $Q_{1,j}$, $|\phi'_j\rangle$, and $|\psi'_j\rangle$ have been defined for each j, $1 \leq j \leq \xi \leq m/2 - 1$, to satisfy

- $\begin{array}{l} |\phi'_1\rangle = V_1|\psi_{\rm init}\rangle, \\ |\phi'_j\rangle = V_j P_{k,j-1} \cdots P_{2,j-1} Q_{1,j-1}|\phi'_{j-1}\rangle, \ 2 \leq j \leq \xi, \\ |\psi'_j\rangle = Q_{1,j}|\phi'_j\rangle, \qquad\qquad\qquad\qquad\quad 1 \leq j \leq \xi. \end{array}$
- $\mathrm{tr}_{\mathcal{P}_1}|\psi_j\rangle\langle\psi_j| = \mathrm{tr}_{\mathcal{P}_1}|\psi'_j\rangle\langle\psi'_j|$, $1 \leq j \leq \xi$.
- All but the first $q_{\rm ent} + 2(j-1)q_{\mathcal{M}}$ qubits in $\mathcal{P}_1$ are the $|0\rangle$-states in the state $|\phi'_j\rangle$.
- All but the first $q_{\rm ent} + 2jq_{\mathcal{M}}$ qubits in $\mathcal{P}_1$ are the $|0\rangle$-states in the state $|\psi'_j\rangle$.

Notice that $Q_{1,1}$, $|\phi'_1\rangle$, and $|\psi'_1\rangle$ defined above satisfy such conditions. Define $Q_{1,\xi+1}$, $|\phi'_{\xi+1}\rangle$, and $|\psi'_{\xi+1}\rangle$ in the following way to satisfy the above four conditions for $j = \xi + 1$.

Let $U_\xi = V_{\xi+1} P_{k,\xi} \cdots P_{2,\xi}$ and define $|\phi'_{\xi+1}\rangle = U_\xi|\psi'_\xi\rangle$. Then all but the first $q_{\rm ent} + 2\xi q_{\mathcal{M}}$ qubits in $\mathcal{P}_1$ are the $|0\rangle$-states in the state $|\phi'_{\xi+1}\rangle$, since none of $P_{2,\xi}, \ldots, P_{k,\xi}, V_{\xi+1}$ acts on the space $\mathcal{P}_1$ and $|\psi'_\xi\rangle$ satisfies the fourth condition. Since $\mathrm{tr}_{\mathcal{P}_1}|\psi_\xi\rangle\langle\psi_\xi| = \mathrm{tr}_{\mathcal{P}_1}|\psi'_\xi\rangle\langle\psi'_\xi|$, by Theorem 7, there exists a unitary transformation A_ξ acting on $\mathcal{P}_1$ such that $A_\xi|\psi'_\xi\rangle = |\psi_\xi\rangle$. Thus we have

$$|\psi_{\xi+1}\rangle = P_{1,\xi+1}U_\xi|\psi_\xi\rangle = P_{1,\xi+1}U_\xi A_\xi|\psi'_\xi\rangle = P_{1,\xi+1}A_\xi U_\xi|\psi'_\xi\rangle = P_{1,\xi+1}A_\xi|\phi'_{\xi+1}\rangle. \tag{2}$$

Hence, by Theorem 10, there exists a state $|\psi'_{\xi+1}\rangle$ such that

$$\mathrm{tr}_{\mathcal{P}_1}|\psi'_{\xi+1}\rangle\langle\psi'_{\xi+1}| = \mathrm{tr}_{\mathcal{P}_1}|\psi_{\xi+1}\rangle\langle\psi_{\xi+1}| \tag{3}$$

and all but the first $q_{\rm ent} + 2(\xi+1)q_{\mathcal{M}}$ qubits in $\mathcal{P}_1$ are the $|0\rangle$-states in the state $|\psi'_{\xi+1}\rangle$. From (2) and (3), we have

$$\mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\psi'_{\xi+1}\rangle\langle\psi'_{\xi+1}| = \mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\psi_{\xi+1}\rangle\langle\psi_{\xi+1}| = \mathrm{tr}_{\mathcal{M}_1 \otimes \mathcal{P}_1}|\phi'_{\xi+1}\rangle\langle\phi'_{\xi+1}|,$$

since $P_{1,\xi+1}$ and A_ξ act only on $\mathcal{M}_1 \otimes \mathcal{P}_1$. Therefore, by Theorem 7, there exists a unitary transformation $Q_{1,\xi+1}$ acting on $\mathcal{M}_1 \otimes \mathcal{P}_1$ such that $Q_{1,\xi+1}|\phi'_{\xi+1}\rangle = |\psi'_{\xi+1}\rangle$. It follows that $Q_{1,\xi+1}$ is of the form $P'_{1,\xi+1} \otimes I_{q_\mathcal{P}-q_{\rm ent}-mq_\mathcal{M}}$, where $P'_{1,\xi+1}$ is a unitary transformation acting on qubits in $\mathcal{M}_1$ and the first $q_{\rm ent}+mq_\mathcal{M}$ qubits of $\mathcal{P}_1$, because all of the last $q_\mathcal{P}-q_{\rm ent}-mq_\mathcal{M}$ qubits in $\mathcal{P}_1$ are the $|0\rangle$-states in both of the states $|\phi'_{\xi+1}\rangle$ and $|\psi'_{\xi+1}\rangle$. One can see that $Q_{1,\xi+1}, |\phi'_{\xi+1}\rangle$, and $|\psi'_{\xi+1}\rangle$ satisfy the four conditions above by their construction.

Having defined $Q_{1,j}, |\phi'_j\rangle, |\psi'_j\rangle$ for each $1 \le j \le m/2$, compare the state just before the final measurement is performed in the original protocol and that in the modified protocol applying $Q_{1,j}$'s instead of $P_{1,j}$'s. For $U_{m/2} = V_{m/2+1}P_{k,m/2}\cdots P_{2,m/2}$, let $|\phi_{m/2+1}\rangle = U_{m/2}|\psi_{m/2}\rangle$ and $|\phi'_{m/2+1}\rangle = U_{m/2}|\psi'_{m/2}\rangle$. These $|\phi_{m/2+1}\rangle$ and $|\phi'_{m/2+1}\rangle$ are exactly the states we want to compare. Noticing that $\mathrm{tr}_{\mathcal{P}_1}|\psi_{m/2}\rangle\langle\psi_{m/2}| = \mathrm{tr}_{\mathcal{P}_1}|\psi'_{m/2}\rangle\langle\psi'_{m/2}|$, we have $\mathrm{tr}_{\mathcal{P}_1}|\phi_{m/2+1}\rangle\langle\phi_{m/2+1}| = \mathrm{tr}_{\mathcal{P}_1}|\phi'_{m/2+1}\rangle\langle\phi'_{m/2+1}|$, since none of $P_{2,m/2},\ldots,P_{k,m/2}, V_{m/2+1}$ acts on $\mathcal{P}_1$. Thus we have

$$\mathrm{tr}_{\mathcal{P}_1\otimes\cdots\otimes\mathcal{P}_k}|\phi_{m/2+1}\rangle\langle\phi_{m/2+1}| = \mathrm{tr}_{\mathcal{P}_1\otimes\cdots\otimes\mathcal{P}_k}|\phi'_{m/2+1}\rangle\langle\phi'_{m/2+1}|,$$

which implies that the verifier V cannot distinguish $|\phi'_{m/2+1}\rangle$ from $|\phi_{m/2+1}\rangle$ at all. Hence, for every input x, the probability of accepting x in the protocol $(Q_1, P_2, \ldots, P_k, V)$ is exactly equal to the one in the original protocol $(P_1,\ldots,P_k,V)$, and Q_1 uses only $q_{\rm ent}+mq_\mathcal{M} = q_{\rm ent}+2\cdot(m/2)\cdot q_\mathcal{M}$ qubits in his private space. In the protocol $(Q_1, P_2, \ldots, P_k, V)$, each $Q_{1,j}$ is described as $Q_{1,j} = P'_{1,j}\otimes I_{q_\mathcal{P}-q_{\rm ent}-mq_\mathcal{M}}$, where $P'_{1,\xi+1}$ is a unitary transformation acting on qubits in $\mathcal{M}_1$ and the first $q_{\rm ent}+mq_\mathcal{M}$ qubits of $\mathcal{P}_1$. Consequently, by constructing an m-message $(q_\mathcal{M}, q_{\rm ent}+mq_\mathcal{M})$-restricted quantum prover P'_1 from each $P'_{1,j}$, for every input x, the probability of accepting x in the protocol $(P'_1, P_2, \ldots, P_k, V)$ is exactly equal to the one in the original protocol $(P_1,\ldots,P_k,V)$.

Now we repeat the above process for each of provers, and finally we obtain a protocol $(P'_1,\ldots,P'_k,V)$ in which all k provers are m-message $(q_\mathcal{M}, q_{\rm ent}+mq_\mathcal{M})$-restricted quantum provers. It is obvious that, for every input x, the probability of accepting x in the protocol $(P'_1,\ldots,P'_k,V)$ is exactly equal to the one in the original protocol $(P_1,\ldots,P_k,V)$, and we have the assertion. □

From Lemma 11, it is straightforward to show the following lemma.

Lemma 12 *For any polynomially bounded functions $k, m, q_{\rm ent}\colon \mathbb{Z}^+ \to \mathbb{N}$, $\mathrm{QMIP}(k, m, q_{\rm ent}, 1, 1/2) \subseteq$ NEXP.*

Proof. For convenience, we assume that the values of m are even (odd cases can be dealt with a similar argument).

Let L be a language in $\mathrm{QMIP}(k, m, q_{\rm ent}, 1, 1/2)$. Then, from Definition 1 together with Lemma 11, there exist polynomially bounded functions $q_\mathcal{V}, q_\mathcal{M}\colon \mathbb{Z}^+ \to \mathbb{N}$ and an m-message $(q_\mathcal{V}, q_\mathcal{M})$-restricted quantum verifier V for a quantum k-prover interactive proof system such that, for every input x, (i) if x is in L, there exists a set of k quantum provers $P_1,\ldots,P_k$ of m-message $(q_\mathcal{M}, q_{\rm ent}+mq_\mathcal{M})$-restricted $q_{\rm ent}$-prior-entangled such that $(P_1,\ldots,P_k,V)$ accepts x with certainty, and (ii) if x is not in L, for all sets of k quantum provers $P'_1,\ldots,P'_k$ of m-message $(q_\mathcal{M}, q_{\rm ent}+mq_\mathcal{M})$-restricted $q_{\rm ent}$-prior-entangled, $(P'_1,\ldots,P'_k,V)$ accepts x with probability at most $1/2$.

For an input x of length n, consider a classical simulation of this quantum k-prover interactive proof system by a non-deterministic Turing machine. Let p_1 be arbitrary fixed polynomial. First, for the initial state $|\psi_{\rm init}\rangle$, an approximation $|\widetilde{\psi}_{\rm init}\rangle$ of $|\psi_{\rm init}\rangle$ can be guessed in time non-deterministic exponential in n with accuracy of $\||\widetilde{\psi}_{\rm init}\rangle - |\psi_{\rm init}\rangle\| < 2^{-p_1(n)}$. Next, since each V_j applied in the original proof system is polynomial-time uniformly generated and $q_\mathcal{V}$ and $q_\mathcal{M}$ are polynomially bounded functions, it is routine to show that an approximation $\widetilde{V}_j$ of a matrix description of V_j can be computed in time exponential in n with accuracy of $\|\widetilde{V}_j - V_j\| < 2^{-p_1(n)}$. Finally, since $q_\mathcal{M}$ and $q_\mathcal{P} = q_{\rm ent}+mq_\mathcal{M}$ are polynomially bounded functions, for each operation $P_{i,j}$ of the ith prover applied in the original

proof system, an approximation $\widetilde{P}_{i,j}$ of a matrix description of $P_{i,j}$ can be guessed in time non-deterministic exponential in n with accuracy of $\|\widetilde{P}_{i,j} - P_{i,j}\| < 2^{-p_1(n)}$. Thus, for the quantum state

$$|\psi_{\text{final}}\rangle = V_{m/2+1}P_{k,m/2}\cdots P_{1,m/2}V_{m/2}\cdots P_{k,1}\cdots P_{1,1}V_1|\psi_{\text{init}}\rangle,$$

which is the state just before the final measurement in the proof system, the approximation $|\widetilde{\psi}_{\text{final}}\rangle$ of $|\psi_{\text{final}}\rangle$ can be computed in time non-deterministic exponential in n with accuracy of $\||\widetilde{\psi}_{\text{final}}\rangle - |\psi_{\text{final}}\rangle\| < 2^{-p_2(n)}$ for any fixed polynomial p_2 by appropriately choosing p_1.

Now, after having computed $|\widetilde{\psi}_{\text{final}}\rangle$, a measurement of the output qubit is simulated by summing up squares of the computed amplitudes in the accepting states. The input x is accepted if and only if this sum, the computed probability that the measurement results in $|1\rangle$, is more than $1-\varepsilon$. From the property of the original proof system, this computed probability is more than $1 - 2^{-2p_2(n)}$ if x is in L, while it is less than $1/2 + 2^{-2p_2(n)}$ if x is not in L. Thus, taking $p_2 = n$ and $\varepsilon = 2^{-2n}$, the input x is accepted if and only if x is in L and the whole computation is done in time non-deterministic exponential in n. □

Hence we have the following theorem.

Theorem 13 $\text{QMIP}^{(\text{l.e.})} \subseteq \text{NEXP}$.

Note that our upper bound of NEXP holds even if we allow protocols with two-sided bounded error, since the proof of Lemma 11 does not depend on the accepting probabilities a, b, and the proof of Lemma 12 can be easily modified to two-sided bounded error cases.

5 $\text{QMIP}^{(\text{n.e.})} = \text{QOC} = \text{NEXP}$

In the previous section, we proved that the class of languages having quantum multi-prover interactive proof systems is necessarily contained in NEXP under the assumption that provers are allowed to share at most polynomially many prior-entangled qubits. As a special case of this, it is proved in this section that, if provers do not share any prior entanglement with each other, the class of languages having quantum multi-prover interactive proof systems is equal to NEXP. Another result related to this is that QOC is also equal to NEXP, or in other words, the class of languages having quantum single-prover interactive proof systems is also equal to NEXP if a prover does not have his private qubits.

The inclusions $\text{QMIP}^{(\text{n.e.})} \subseteq \text{NEXP}$ and $\text{QOC} \subseteq \text{NEXP}$ directly come from Lemma 12. Thus it is sufficient for our claim to show $\text{NEXP} \subseteq \text{QMIP}^{(\text{n.e.})} \subseteq \text{QOC}$. Fortunately, in the cases without prior entanglement, it is easy to show that a quantum verifier can successfully simulate any classical multi-prover protocol, in particular, a one-round two-prover classical interactive protocol that can verify a language in NEXP with exponentially small one-sided error [15]. Thus, we have the following theorem and corollary. The proof of Theorem 14 is straightforward, and thus omitted here (see Appendix A).

Theorem 14 $\text{NEXP} \subseteq \text{QMIP}^{(\text{n.e.})}$.

Corollary 15 *For prior unentangled cases, if a language L has a quantum multi-prover interactive proof system with two-sided bounded error, then L has a two-message quantum two-prover interactive proof system with exponentially small one-sided error.*

The remainder of this section is devoted to the proof of $\text{QMIP}^{(\text{n.e.})} \subseteq \text{QOC}$.

Lemma 16 *Let $k, m\colon \mathbb{Z}^+ \to \mathbb{N}$ be polynomially bounded functions, and $a, b\colon \mathbb{Z}^+ \to [0,1]$ be functions satisfying $a \geq b$. Then* $\text{QMIP}(k, m, 0, a, b) \subseteq \text{QOC}(k\lfloor (m+1)/2 \rfloor, a, b)$.

Proof. For simplicity, we assume that the values of m are even, and thus $k\lfloor (m+1)/2 \rfloor = km/2$ (odd cases can be proved with a similar argument).

Let L be a language in QMIP$(k, m, 0, a, b)$. Then, from Definition 1 together with Lemma 11, there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and an m-message $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V for a quantum k-prover interactive proof system such that, for every input x of length n, (i) if x is in L, there exists a set of m-message $(q_{\mathcal{M}}, mq_{\mathcal{M}})$-restricted quantum provers $P_1, \ldots, P_k$ without prior entanglement such that $(P_1, \ldots, P_k, V)$ accepts x with probability at least $a(n)$, and (ii) if x is not in L, for all sets of m-message $(q_{\mathcal{M}}, mq_{\mathcal{M}})$-restricted quantum provers $P'_1, \ldots, P'_k$ without prior entanglement, $(P'_1, \ldots, P'_k, V)$ accepts x with probability at most $b(n)$.

We construct a $km/2$-oracle-call verifier V^{QOC} of a quantum oracle circuit as follows. Let us consider that quantum registers (collections of qubits upon which various transformations are performed) $\mathbf{W}$, $\mathbf{M}_i$, and $\mathbf{P}_i$, for $1 \leq i \leq k$, are prepared among the private qubits of the verifier V^{QOC}, and quantum registers $\mathbf{M}$ and $\mathbf{P}$ are prepared among the qubits for oracle calls. $\mathbf{W}$ consists of $q_{\mathcal{V}}$ qubits, each $\mathbf{M}_i$ and $\mathbf{M}$ consist of $q_{\mathcal{M}}$ qubits, and each $\mathbf{P}_i$ and $\mathbf{P}$ consist of $q_{\mathcal{P}} = mq_{\mathcal{M}}$ qubits. Let $\mathcal{W}^{\mathrm{QOC}}$, each $\mathcal{M}_i^{\mathrm{QOC}}$, and each $\mathcal{P}_i^{\mathrm{QOC}}$ denote the Hilbert spaces corresponding to the registers $\mathbf{W}$, $\mathbf{M}_i$, and $\mathbf{P}_i$, respectively. Take the Hilbert space $\mathcal{V}^{\mathrm{QOC}}$ corresponding to the qubits private to the verifier V^{QOC} as $\mathcal{V}^{\mathrm{QOC}} = \mathcal{W}^{\mathrm{QOC}} \otimes \mathcal{M}_1^{\mathrm{QOC}} \otimes \cdots \otimes \mathcal{M}_k^{\mathrm{QOC}} \otimes \mathcal{P}_1^{\mathrm{QOC}} \otimes \cdots \otimes \mathcal{P}_k^{\mathrm{QOC}}$. Accordingly, the number of private qubits of V^{QOC} is $q_{\mathcal{V}}^{\mathrm{QOC}} = q_{\mathcal{V}} + k(q_{\mathcal{M}} + q_{\mathcal{P}}) = q_{\mathcal{V}} + k(m+1)q_{\mathcal{M}}$. Let $\mathcal{M}^{\mathrm{QOC}}$ and $\mathcal{P}^{\mathrm{QOC}}$ denote the Hilbert spaces corresponding to the registers $\mathbf{M}$ and $\mathbf{P}$, respectively. Take the Hilbert space $\mathcal{O}^{\mathrm{QOC}}$ corresponding to the qubits for oracle calls as $\mathcal{O}^{\mathrm{QOC}} = \mathcal{M}^{\mathrm{QOC}} \otimes \mathcal{P}^{\mathrm{QOC}}$. Accordingly, the number of qubits for oracle calls is $q_{\mathcal{O}}^{\mathrm{QOC}} = q_{\mathcal{M}} + q_{\mathcal{P}} = (m+1)q_{\mathcal{M}}$.

Consider each V_j, the jth quantum circuit of the verifier V of the original quantum k-prover interactive proof system, which acts on $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k$. For each j, let U_j^{QOC} be just the same unitary transformation as V_j and U_j^{QOC} acts on $\mathcal{W}^{\mathrm{QOC}} \otimes \mathcal{M}_1^{\mathrm{QOC}} \otimes \cdots \otimes \mathcal{M}_k^{\mathrm{QOC}}$, corresponding to that V_j acts on $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k$. Define the verifier V^{QOC} of the corresponding quantum oracle circuit in the following way:

- At the first transformation of V^{QOC}, V^{QOC} first applies U_1^{QOC}, and then swaps the contents of $\mathbf{M}_1$ for those of $\mathbf{M}$.
- At the $((j-1)k+1)$-th transformation of V^{QOC} for each $2 \leq j \leq m/2$, V^{QOC} first swaps the contents of $\mathbf{M}$ and $\mathbf{P}$ for those of $\mathbf{M}_k$ and $\mathbf{P}_k$, respectively, then applies U_j^{QOC}, and finally swaps the contents of $\mathbf{M}_1$ and $\mathbf{P}_1$ for those of $\mathbf{M}$ and $\mathbf{P}$.
- At the $((j-1)k+i)$-th transformation of V^{QOC} for each $2 \leq i \leq k, 1 \leq j \leq m/2$, V^{QOC} first swaps the contents of $\mathbf{M}$ and $\mathbf{P}$ for those of $\mathbf{M}_{i-1}$ and $\mathbf{P}_{i-1}$, respectively, then swaps the contents of $\mathbf{M}_i$ and $\mathbf{P}_i$ for those of $\mathbf{M}$ and $\mathbf{P}$.

(i) In the case the input x of length n is in L:
In the original m-message quantum k-prover interactive proof system, there exist m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted prior-unentangled quantum provers $P_1, \ldots, P_k$ that cause V to accept x with probability at least $a(n)$. Hence, if we let $O_{(j-1)k+i}$ for each $1 \leq i \leq k, 1 \leq j \leq m/2$ be just the same unitary transformation as $P_{i,j}$ ($O_{(j-1)k+i}$ acts on $\mathcal{O}^{\mathrm{QOC}} = \mathcal{M}^{\mathrm{QOC}} \otimes \mathcal{P}^{\mathrm{QOC}}$ corresponding to that $P_{i,j}$ acts on $\mathcal{M}_i \otimes \mathcal{P}_i$), it is obvious that the probability of accepting x by V^{QOC} with access to O is exactly equal to the one the original V accepts it, which is at least $a(n)$.

(ii) In the case the input x of length n is not in L:
Suppose that there were an oracle O' that makes the verifier V^{QOC} accept x with probability more than $b(n)$. Consider m-message $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted prior-unentangled provers $P'_1, \ldots, P'_k$ of the original m-message quantum k-prover interactive proof system such that, for each $1 \leq i \leq k, 1 \leq j \leq m/2$, $P'_{i,j}$ is just the same transformation as $O'_{(j-1)k+i}$ ($P'_{i,j}$ acts on $\mathcal{M}_i \otimes \mathcal{P}_i$

corresponding to that $O'_{(j-1)k+i}$ acts on $\mathcal{M}^{\mathrm{QOC}} \otimes \mathcal{P}^{\mathrm{QOC}}$). By their construction, it is obvious that the probability with which these provers $P'_1, \ldots, P'_k$ can convince the verifier V is exactly equal to the one with which the oracle O' can, which is more than $b(n)$. This contradicts the assumption.

□

The inclusion $\mathrm{QMIP}^{(\mathrm{n.e.})} \subseteq \mathrm{QOC}$ immediately follows from Lemma 16. Thus we have the following theorem.

Theorem 17 $\mathrm{QMIP}^{(\mathrm{n.e.})} = \mathrm{QOC} = \mathrm{NEXP}$.

6 Conclusions and Open Problems

This paper analyzed the power of quantum multi-prover interactive proof systems and gave the NEXP upper bound for them in the cases that provers share at most polynomially many prior-entangled qubits. In particular, if provers do not share any prior entanglement with each other, the class of languages having quantum multi-prover interactive proof systems was shown equal to NEXP. Related to these, if a prover does not have his private qubits, the class of languages having quantum single-prover interactive proof systems was also shown equal to NEXP.

A number of interesting problems remain open regarding quantum interactive proof systems.

- We know very little about the power of general quantum multi-prover interactive proof systems with provers sharing arbitrarily many prior-entangled qubits. Can exponentially many prior-entangled qubits among provers help a quantum verifier to verify a language not in NEXP? Does NEXP have quantum multi-prover interactive proof systems with prior-entangled provers?
- Probabilistic oracle machines are closely related to the theory of probabilistic checkable proofs [3, 2]. How is the relation between the quantum oracle circuits introduced in this paper and possible quantum analogues of probabilistic checkable proofs?
- In the classical setting the power of one-message multi-prover interactive proof systems obviously remains same as that of one-message single-prover ones. However, as Kobayashi, Matsumoto, and Yamakami [24] noticed, it might not be so in the quantum setting. How is the power of one-message quantum multi-prover interactive proof systems (both in the cases with and without prior entanglement)?

Acknowledgements

The authors are grateful to Richard E. Cleve for explaining how an entangled pair of provers can cheat a classical verifier in some cases, and Lance J. Fortnow for his valuable comments on writing this paper. The authors would also like to thank Hiroshi Imai for his comments and support.

References

[1] 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.

[2] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998. Preliminary version entitled "Proof verification and hardness of approximation problems" appeared in *33rd Annual Symposium on Foundations of Computer Science*, pages 14–22, 1992.

[3] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.
Preliminary version appeared in *33rd Annual Symposium on Foundations of Computer Science*, pages 2–13, 1992.

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

[5] László Babai, Lance J. Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.
Preliminary version appeared in *31st Annual Symposium on Foundations of Computer Science*, volume I, pages 16–25, 1990.

[6] Mihir Bellare, Uriel Feige, and Joe Kilian. On the role of shared randomness in two prover proof systems. In *Third Israel Symposium on the Theory of Computing and Systems*, pages 199–208, 1995.

[7] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.

[8] 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.

[9] 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.

[10] Jin-Yi Cai, Anne Condon, and Richard J. Lipton. On bounded round multi-prover interactive proof systems. In *Proceedings, Structure in Complexity Theory, Fifth Annual Conference*, pages 45–54, 1990.

[11] Jin-Yi Cai, Anne Condon, and Richard J. Lipton. PSPACE is provable by two provers in one round. *Journal of Computer and System Sciences*, 48(1):183–193, 1994.
Preliminary version appeared in *Proceedings, Structure in Complexity Theory, Sixth Annual Conference*, pages 110–115, 1991.

[12] Richard E. Cleve. An entangled pair of provers can cheat. Talk at the Workshop on Quantum Computation and Information, California Institute of Technology, November 2000.

[13] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London, Series A*, 400:97–117, 1985.

[14] Uriel Feige. On the success probability of two provers in one-round proof systems. In *Proceedings, Structure in Complexity Theory, Sixth Annual Conference*, pages 116–123, 1991.

[15] Uriel Feige and László Lovász. Two-prover one-round proof systems: Their power and their problems (extended abstract). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on the Theory of Computing*, pages 733–744, 1992.

[16] Lance J. Fortnow. *Complexity-Theoretic Aspects of Interactive Proof Systems*. PhD thesis, Department of Mathematics, Massachusetts Institute of Technology, May 1989.

[17] 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.

[18] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.
Preliminary version appeared in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[19] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In Silvio Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. JAI Press, 1989.
Preliminary version appeared in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, pages 59–68, 1986.

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

[21] Lane P. Hughston, Richard O. Jozsa, and William K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14–18, 1993.

[22] 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.

[23] 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.

[24] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? Los Alamos e-print archive, quant-ph/0306051, 2003.

[25] Dror Lapidot and Adi Shamir. Fully parallelized multi-prover protocols for NEXP-time. *Journal of Computer and System Sciences*, 54(2):215–220, 1997.
Preliminary version appeared in *32nd Annual Symposium on Foundations of Computer Science*, pages 13–18, 1991.

[26] Carsten Lund, Lance J. Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.
Preliminary version appeared in *31st Annual Symposium on Foundations of Computer Science*, volume I, pages 2–10, 1990.

[27] Michael A. Nielsen. Entanglement and distributed quantum computation. Talk at the 4th Workshop on Quantum Information Processing, Amsterdam, January 2001.

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

[29] Christos H. Papadimitriou. Games against nature. *Journal of Computer and System Sciences*, 31(2):288–301, 1985.
Preliminary version appeared in *24th Annual Symposium on Foundations of Computer Science*, pages 446–450, 1983.

[30] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.
Preliminary version appeared in *31st Annual Symposium on Foundations of Computer Science*, volume I, pages 11–15, 1990.

[31] Alexander H. Shen. IP = PSPACE: Simplified proof. *Journal of the ACM*, 39(4):878–880, 1992.

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

[33] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
Preliminary version entitled "Algorithms for quantum computation: Discrete logarithms and factoring," appeared in *35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[34] Armin Uhlmann. Parallel transport and "quantum holonomy" along density operators. *Reports on Mathematical Physics*, 24:229–240, 1986.

[35] John H. Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.
Preliminary version appeared in *40th Annual Symposium on Foundations of Computer Science*, pages 112–119, 1999.

Appendix

A Proof of Theorem 14

It is known that every language in NEXP has a (classical) multi-prover interactive proof system, in particular, a one-round two-prover classical interactive proof system with exponentially small one-sided error [15]. Under the assumption that provers do not share any prior entanglement with each other, it is easy to show that a quantum verifier can successfully simulate such a classical one-round two-prover protocol (cf. [12]).

Proof of Theorem 14. Given a classical k-prover interactive protocol, consider such a quantum k-prover protocol without prior entanglement that a quantum verifier performs measurements in $\{|0\rangle, |1\rangle\}$ basis on every qubit of his part at every time he sends questions to quantum provers and at every time he receives responses from them, and for the rest part of computation the quantum verifier behaves in the same manner as the classical verifier does. Such a protocol can be simulated without intermediate measurements by only using unitary transformations [1, 20]. Furthermore, since there is no prior entanglement among private qubits of the quantum provers, such a quantum protocol makes no difference from a classical protocol in which a classical verifier chooses a set of k classical provers probabilistically at the beginning of the protocol. Therefore, in such a quantum k-prover protocol, for every input, the quantum provers can be only as powerful as the classical provers, i.e., the quantum provers can behave just in the same way as the classical provers do, while no set of k quantum provers can convince the quantum verifier with probability more than the maximum probability with which a set of k classical provers can convince the classical verifier.

Now we explain in more detail. Let L be a language in NEXP, then L has a one-round two-prover interactive proof system. Let V be the classical verifier of this one-round two-prover interactive proof system. We construct a two-message quantum two-prover interactive proof system by just simulating this classical protocol.

Assume that, just after the classical verifier V has sent questions to the provers P_1 and P_2, the contents of V's private tape, the question to P_1, and the question to P_2 are v, q_1, and q_2, respectively, with probability $p(v, q_1, q_2)$. Our two-message quantum verifier $V^{(\mathrm{Q})}$ prepares the quantum registers $\mathbf{V}$, $\mathbf{Q}_1$, $\mathbf{Q}_2$, $\mathbf{A}_1$, and $\mathbf{A}_2$ among his private qubits. $V^{(\mathrm{Q})}$ first stores v, q_1, and q_2 in $\mathbf{V}$, $\mathbf{Q}_1$, and $\mathbf{Q}_2$,

respectively, then copies the contents of each $\mathbf{Q}_i$ to the message qubits shared with a quantum prover $P_i^{(\mathrm{Q})}$. That is, $V^{(\mathrm{Q})}$ prepares the superposition

$$\sum_{v,q_1,q_2} \Big(\sqrt{p(v,q_1,q_2)} \underbrace{|v\rangle}_{\mathbf{V}} \underbrace{|q_1\rangle}_{\mathbf{Q}_1} \underbrace{|q_2\rangle}_{\mathbf{Q}_2} \underbrace{|0\rangle}_{\mathbf{A}_1} \underbrace{|0\rangle}_{\mathbf{A}_2} \underbrace{|q_1\rangle}_{\mathbf{M}_1} \underbrace{|0\rangle}_{\mathbf{P}_1} \underbrace{|q_2\rangle}_{\mathbf{M}_2} \underbrace{|0\rangle}_{\mathbf{P}_2} \Big),$$

where, for each $i = 1, 2$, $\mathbf{M}_i$ denotes the quantum register that consists of the message qubits between $V^{(\mathrm{Q})}$ and $P_i^{(\mathrm{Q})}$, and $\mathbf{P}_i$ denotes the quantum register that consists of $P_i^{(\mathrm{Q})}$'s private qubits.

Next the quantum provers $P_1^{(\mathrm{Q})}$ and $P_2^{(\mathrm{Q})}$ apply some unitary transformations on their qubits. Now the state becomes

$$\begin{aligned}
&\sum_{v,q_1,q_2} \Bigg\{ \sqrt{p(v,q_1,q_2)} \underbrace{|v\rangle}_{\mathbf{V}} \underbrace{|q_1\rangle}_{\mathbf{Q}_1} \underbrace{|q_2\rangle}_{\mathbf{Q}_2} \underbrace{|0\rangle}_{\mathbf{A}_1} \underbrace{|0\rangle}_{\mathbf{A}_2} \\
&\qquad \otimes \Big(\sum_{a_1} \alpha_1(q_1,a_1) \underbrace{|a_1\rangle}_{\mathbf{M}_1} \underbrace{|\psi_1(q_1,a_1)\rangle}_{\mathbf{P}_1} \Big) \otimes \Big(\sum_{a_2} \alpha_2(q_2,a_2) \underbrace{|a_2\rangle}_{\mathbf{M}_2} \underbrace{|\psi_2(q_2,a_2)\rangle}_{\mathbf{P}_2} \Big) \Bigg\} \\
&= \sum_{v,q_1,q_2,a_1,a_2} \Big(\sqrt{p(v,q_1,q_2)} \alpha_1(q_1,a_1) \alpha_2(q_2,a_2) \\
&\qquad \times \underbrace{|v\rangle}_{\mathbf{V}} \underbrace{|q_1\rangle}_{\mathbf{Q}_1} \underbrace{|q_2\rangle}_{\mathbf{Q}_2} \underbrace{|0\rangle}_{\mathbf{A}_1} \underbrace{|0\rangle}_{\mathbf{A}_2} \underbrace{|a_1\rangle}_{\mathbf{M}_1} \underbrace{|\psi_1(q_1,a_1)\rangle}_{\mathbf{P}_1} \underbrace{|a_2\rangle}_{\mathbf{M}_2} \underbrace{|\psi_2(q_2,a_2)\rangle}_{\mathbf{P}_2} \Big),
\end{aligned}$$

where each $\alpha_i(q_i, a_i)$ denotes the transition amplitude and each $|\psi_i(q_i, a_i)\rangle$ is a unit vector in the private space of $P_i^{(\mathrm{Q})}$.

Finally, $V^{(\mathrm{Q})}$ copies the contents of the message qubits shared with the quantum prover $P_i^{(\mathrm{Q})}$ to $\mathbf{A}_i$ to have the following state

$$\sum_{v,q_1,q_2,a_1,a_2} \Big(\sqrt{p(v,q_1,q_2)} \alpha_1(q_1,a_1) \alpha_2(q_2,a_2) \underbrace{|v\rangle}_{\mathbf{V}} \underbrace{|q_1\rangle}_{\mathbf{Q}_1} \underbrace{|q_2\rangle}_{\mathbf{Q}_2} \underbrace{|a_1\rangle}_{\mathbf{A}_1} \underbrace{|a_2\rangle}_{\mathbf{A}_2} \underbrace{|a_1\rangle}_{\mathbf{M}_1} \underbrace{|\psi_1(q_1,a_1)\rangle}_{\mathbf{P}_1} \underbrace{|a_2\rangle}_{\mathbf{M}_2} \underbrace{|\psi_2(q_2,a_2)\rangle}_{\mathbf{P}_2} \Big),$$

and does just the same computation as the classical verifier V using $\mathbf{V}$, $\mathbf{M}_1$ and $\mathbf{M}_2$. $V^{(\mathrm{Q})}$ accepts the input if and only if V accepts it.

(i) In the case the input x of length n is in L:
The quantum provers have only to answer in just the same way as the classical provers do, and $V^{(\mathrm{Q})}$ accepts x with probability 1.

(ii) In the case the input x of length n is not in L:
Since no quantum interference occurs among the computational paths with different 4-tuple (q_1, q_2, a_1, a_2), and from the fact that any pair of classical provers cannot convince the classical verifier with probability more than 1/2 (actually $1/2^n$), it is obvious that, for any pair of quantum provers, $V^{(\mathrm{Q})}$ accepts x with probability at most 1/2 (actually $1/2^n$).

□