CHICAGO JOURNAL OF THEORETICAL COMPUTER SCIENCE 2012, Article 09, pages 1–10
http://cjtcs.cs.uchicago.edu/

On Quantum Interactive Proofs with Short Messages

Attila Pereszlényi

Received: June 4, 2012; revised: October 19, 2012 and November 30, 2012; published: December 1, 2012.

Abstract: This paper proves one of the open problems posed by Beigi, Shor and Watrous in [*ToC*, Volume 7, Article 7, pp. 101–117, 2011]. We consider quantum interactive proof systems where, in the beginning, the verifier and prover send messages to each other, with the combined length of all messages being at most logarithmic (in the input length); and at the end, the prover sends a polynomial-length message to the verifier. We show that this class has the same expressive power as QMA.

1 Introduction

Quantum interactive proof systems (QIP) were introduced by Watrous [16] as a natural extension of interactive proofs (IP) to the quantum computational setting. They have been extensively studied and now it's known that the power of quantum interactive proof systems is the same as that of the classical ones, i. e., QIP = IP = PSPACE [12, 15, 7]. Furthermore, quantum interactive proof systems still have the same expressive power if we restrict the number of messages to three and have exponentially small one-sided error [10]. If the interaction is only one message from the prover to the verifier then the class is called QMA, which is the quantum analogue of NP and MA. QMA can also be made to have exponentially small error, and has natural complete problems [1].

Several variants of QIP and QMA have also been studied. We now focus on the case where some or all of the messages are small, meaning at most logarithmic in the input length. These cases are usually not interesting in the classical setting since a logarithmic-length message can be eliminated by the verifier by enumerating all possibilities. This is not true in the quantum case. Indeed, a variant of QMA that uses two unentangled, logarithmic-length proofs contains NP [3]; hence not believed to be equal to BQP. On

Key words and phrases: interactive proof systems, Merlin-Arthur proof systems, quantum computing

DOI: 10.4086/cjtcs.2012.009

the other hand, if QMA has one logarithmic-length proof then it has the same expressive power as BQP [13].

Beigi et al. [2] proved that in other variants of quantum interactive proof systems the short message can also be eliminated without changing the power of the proof system. Besides other results, they showed that in the setting when the verifier sends a short message to the prover and the prover responds with an ordinary, polynomial-length message, the short message can be discarded, and hence the class has the same power as QMA. They have raised the question if this is also true if we replace the short question of the verifier with a 'short interaction', i. e., consider quantum interactive proof systems where in the beginning the verifier and prover send messages to each other with the combined length of all messages being at most logarithmic, and at the end the prover sends a polynomial-length message to the verifier. We show that this class has the same power as QMA, or in other words, the short interaction can be discarded. This is formalized by the following theorem.

Theorem 1.1. *Let $c,s : \mathbb{N} \to (0,1)$ be polynomial-time computable functions such that $c(n) - s(n) \in 1/\mathsf{poly}(n)$. Then $\mathsf{QIP}_{\text{short}}(O(\log n), c, s) = \mathsf{QMA}$.*

Here $\mathsf{QIP}_{\text{short}}(O(\log n), c, s)$ is the class described above, with completeness-soundness gap being separated by some inverse-polynomial function of the input length. For a rigorous description of the class see Definition 2.1.

1.1 The Idea Behind the Proof of Theorem 1.1

We observe that it's sufficient for the QIP prover to have only $O(\log n)$ qubits in its private work register in all but the last round without changing the acceptance probability. So the prover's unitaries in these rounds can be approximated by polynomial-size quantum circuits. The prover in the QMA proof system gives the classical descriptions of these circuits to the verifier who approximately produces the state of the whole system appearing in the beginning of the last round of the QIP protocol. This system is composed of the prover's private space, the question to the prover and the verifier's private space. While simulating the last round, we don't care about the prover's private space, so we treat its operation as a quantum channel whose input is the private space of the prover and the question from the verifier, and whose output is the answer to the verifier. Since the input is on $O(\log n)$-many qubits, to perform the action of this channel, we can use the same method as in [2, Section 3]. For this step the QMA prover sends many copies of the normalized Choi-Jamiołkowski representation of the channel, with which the verifier can simulate the channel using 'post-selection'.

Organization of the Paper

The remainder of the paper is organized as follows. Section 2 discusses the background theorems and definitions needed for the proof of our main theorem. The proof itself is presented in Section 3. We end the paper with a description of an open problem in Section 4.

2 Preliminaries

We assume familiarity with quantum information [18], computation [14] and computational complexity [17]; such as mixed states, unitary operations, quantum channels, representations of quantum channels, quantum de Finetti theorems, state tomography and complexity classes like QMA and QIP. The purpose of this section is to present the notations and background information (definitions, theorems) required to understand the rest of the paper.

We denote the set of positive functions of n that are upper-bounded by some polynomial in n by $\mathsf{poly}(n)$. If the argument is clear, we omit it and just write poly. We try to follow the notations used in [18, 2]. When we talk about a quantum register (R) of size k, we mean the object made up of k qubits. It has associated Hilbert space $\mathcal{R} = \mathbb{C}^{2^k}$. $\mathrm{L}(\mathcal{R})$ denotes the space of all linear mappings from $\mathcal{R}$ to itself. The set of all density operators on $\mathcal{R}$ is denoted by $\mathrm{D}(\mathcal{R})$. The adjoint of $\mathbf{X} \in \mathrm{L}(\mathcal{R})$ is denoted by $\mathbf{X}^*$. The trace norm of $\mathbf{X} \in \mathrm{L}(\mathcal{R})$ is defined by

$$\|\mathbf{X}\|_{\mathrm{Tr}} \stackrel{\mathrm{def}}{=} \mathrm{Tr}\left(\sqrt{\mathbf{X}^*\mathbf{X}}\right),$$

and the trace distance between $\mathbf{X}$ and $\mathbf{Y}$ is defined as

$$\frac{1}{2}\|\mathbf{X}-\mathbf{Y}\|_{\mathrm{Tr}}.$$

A quantum channel or super-operator (Φ) is a completely positive and trace-preserving linear map of the form $\Phi : \mathrm{L}(\mathcal{Q}) \to \mathrm{L}(\mathcal{R})$. The set of all such channels is denoted by $\mathrm{C}(\mathcal{Q},\mathcal{R})$. The trace norm of a super-operator $\Phi \in \mathrm{C}(\mathcal{Q},\mathcal{R})$ is defined as

$$\|\Phi\|_{\mathrm{Tr}} \stackrel{\mathrm{def}}{=} \max\left\{\|\Phi(\mathbf{X})\|_{\mathrm{Tr}} \,:\, \mathbf{X} \in \mathrm{L}(\mathcal{Q}), \|\mathbf{X}\|_{\mathrm{Tr}} \leq 1\right\},$$

and the diamond norm of Φ is

$$\|\Phi\|_{\diamond} \stackrel{\mathrm{def}}{=} \left\|\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Q})}\right\|_{\mathrm{Tr}},$$

where $\mathbb{1}_{\mathrm{L}(\mathcal{Q})}$ is the identity super-operator on $\mathrm{L}(\mathcal{Q})$. More on these norms can be found in [18]. For any $\Phi \in \mathrm{C}\left(\mathbb{C}^{2^k}, \mathbb{C}^{2^\ell}\right)$ the normalized Choi-Jamiołkowski representation of Φ is defined to be

$$\rho_\Phi \in \mathrm{D}\left(\mathbb{C}^{2^\ell} \otimes \mathbb{C}^{2^k}\right), \qquad \rho_\Phi \stackrel{\mathrm{def}}{=} \frac{1}{2^k} \sum_{x,y \in \{0,1\}^k} \Phi(|x\rangle\langle y|) \otimes |x\rangle\langle y|.$$

It can be generated by applying Φ on one half of k pairs of qubits in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If we are given ρ_Φ and an arbitrary $\sigma \in \mathrm{D}\left(\mathbb{C}^{2^k}\right)$ then there exists a simple procedure which produces $\Phi(\sigma)$ with probability $1/4^k$. We will refer to it as 'post-selection'. For details see [2, Section 2.1].

When we talk about a polynomial-time quantum algorithm, we mean a quantum circuit containing Hadamard (**H**), $\pi/8$ (**T**) and controlled-not (**CNOT**) gates, and which can be generated by a classical algorithm in polynomial-time. The classes QMA and QIP have been defined in [1] and [16] respectively, and we will use those definitions. Now we want to define the quantum interactive proof systems where in

the beginning there is a $O(\log n)$-long interaction which is followed by a $\mathsf{poly}(n)$-length message from the prover. Note that in this setting we can assume, without loss of generality, that all messages, except the last one, consist of a single qubit, and the total number of rounds is at most $O(\log n)$. This is because we can add dummy qubits that are interspersed with the qubits sent by the other party. We define the class according to this observation.

Definition 2.1. Let the class $\mathsf{QIP}_{\text{short}}(m,c,s)$ be the set of languages for which there exists a quantum interactive proof system with the following properties. The completeness parameter is c and the soundness is s. The proof system consists of m rounds, each round is a question-answer pair. All questions and answers are one qubits except for the last answer which is $\mathsf{poly}(n)$ qubits, where n is the length of the input. See Figure 1 for an example with $m = 3$.

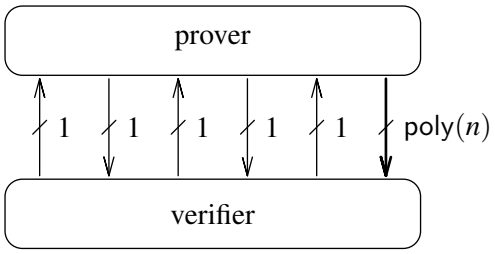

Figure 1: The interaction in the proof system of Definition 2.1 in case $m = 3$.

A similar class, $\mathsf{QIP}([\log,\mathsf{poly}],c,s)$ was defined in [2] to be the class of problems for which there exists a one round quantum interactive proof system, with completeness and soundness parameters c and s. Additionally the verifier's question has length $O(\log n)$, and the prover's answer is $\mathsf{poly}(n)$ qubits.

Remark 2.2. The following inclusion is trivially true between the above classes.

$$\mathsf{QIP}([\log,\mathsf{poly}],c,s) \subseteq \mathsf{QIP}_{\text{short}}(O(\log n),c,s),$$

for all values of c and s.

In [2] it was proven that in their setting the question from the verifier is unnecessary. This is formulated by the following theorem.

Theorem 2.3 ([2])**.** *Let $c,s : \mathbb{N} \to (0,1)$ be polynomial-time computable functions such that $c(n) - s(n) \in 1/\mathsf{poly}(n)$. Then $\mathsf{QIP}([\log,\mathsf{poly}],c,s) = \mathsf{QMA}$.*

In the next section we prove that the seemingly stronger class of Definition 2.1 also has the same power as QMA if $m = O(\log n)$. For this we will need the following theorems.

Lemma 2.4. *Let us have a $\mathsf{QIP}_{\text{short}}(m+1,c,s)$ proof system. Without loss of generality (i. e., without changing completeness c and soundness s) we can assume that during the first m rounds the prover only uses $2m$ qubits in its private register, in both the honest and the dishonest case. Moreover, the actions of the prover in each of these rounds are unitary transformations.*

The above lemma is a special case of [11, Lemma 11] (when there is only one prover), and also appears in the proof of Theorem 6 of [6]. The intuitive reason why it holds is the following. Before the verifier and prover interact, the state of the whole system (i. e., the verifier's and the prover's private spaces) has Schmidt number one. With each qubit sent, the Schmidt number of this system increases at most by a factor of two. At the end of the mth round the Schmidt number of the system is at most 2^{2m}. This means that we can find a purification of the verifier's state, in each step, which has at most $2m$ qubits at the prover's side. For each round we find two purifications; first when the prover receives the question and second after the prover generates the answer. From the "unitary equivalence of purifications" there exist unitary transformations on the prover's side that transform between these purifications. The following theorems will be used to put an upper-bound on the number of gates we need to simulate these unitaries.

Theorem 2.5 ([14], Chapter 4.5.2)**.** *An arbitrary unitary operator on ℓ qubits can be implemented using a circuit containing $O\left(\ell^2 4^\ell\right)$ single qubit and* **CNOT** *gates.*

The next theorem follows from the Solovay-Kitaev theorem [9, 14, 5].

Theorem 2.6. *For any unitary operator $\mathbf{U}$ on one qubit and $\varepsilon > 0$, there exists a circuit $C_{\mathbf{U},\varepsilon}$ such that $C_{\mathbf{U},\varepsilon}$ is made up of $O\left(\log^4(1/\varepsilon)\right)$ gates from the set $\{\mathbf{H},\mathbf{T}\}$, and*

$$\left\|\Phi_{\mathbf{U}} - C_{\mathbf{U},\varepsilon}\right\|_\diamond \leq \varepsilon,$$

where $\Phi_{\mathbf{U}} : \mathrm{L}\left(\mathbb{C}^2\right) \to \mathrm{L}\left(\mathbb{C}^2\right)$ and $\Phi_{\mathbf{U}}(\rho) = \mathbf{U}\rho\mathbf{U}^*$.

The following is corollary to Theorem 2.5 and 2.6.

Corollary 2.7. *For any unitary operator $\mathbf{U}$ on ℓ qubits and $\varepsilon > 0$, there exists a circuit $C_{\mathbf{U},\varepsilon}$ such that $C_{\mathbf{U},\varepsilon}$ is made up of $O\left(5^\ell \cdot \log^4\left(5^\ell/\varepsilon\right)\right)$ gates from the set $\{\mathbf{H},\mathbf{T},\mathbf{CNOT}\}$, and*

$$\left\|\Phi_{\mathbf{U}} - C_{\mathbf{U},\varepsilon}\right\|_\diamond \leq \varepsilon,$$

where $\Phi_{\mathbf{U}} : \mathrm{L}\left(\mathbb{C}^{2^\ell}\right) \to \mathrm{L}\left(\mathbb{C}^{2^\ell}\right)$ and $\Phi_{\mathbf{U}}(\rho) = \mathbf{U}\rho\mathbf{U}^*$.

Corollary 2.8. *Let $\Phi_{\mathbf{U}}$ and $C_{\mathbf{U},\varepsilon}$ be given by Corollary 2.7, and let $\mathcal{H}$ be an arbitrary finite dimensional complex Euclidean space. From the properties of the diamond norm, it follows that for all $\rho \in \mathrm{D}\left(\mathbb{C}^{2^\ell} \otimes \mathcal{H}\right)$,*

$$\left\|\left(\Phi_{\mathbf{U}} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{H})}\right)(\rho) - \left(C_{\mathbf{U},\varepsilon} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{H})}\right)(\rho)\right\|_{\mathrm{Tr}} \leq \varepsilon.$$

The following claims will be used in the discussion of how the verifier simulates the last round.

Lemma 2.9 (Lemma 1 of [2])**.** *Let $\rho \in \mathrm{D}\left(\mathbb{C}^{2^q}\right)$ be a state on $q = O(\log n)$ qubits. For any $\varepsilon \in 1/\mathsf{poly}(n)$, choose N such that $N \geq 2^{10q}/\varepsilon^3$ and $N \in \mathsf{poly}(n)$. If $\rho^{\otimes N}$ is given to a $\mathsf{poly}(n)$-time quantum machine, then it can perform quantum state tomography, and get a classical description $\xi \in \mathrm{L}\left(\mathbb{C}^{2^q}\right)$ of ρ, which with probability at least $1-\varepsilon$ satisfies*

$$\left\|\rho - \xi\right\|_{\mathrm{Tr}} < \varepsilon.$$

Theorem 2.10 (quantum de Finetti theorem [4]; this form is from [18])**.** *Let* $\mathsf{X}_1,\ldots,\mathsf{X}_n$ *be identical quantum registers, each having associated space* $\mathbb{C}^d$*, and let* $\rho \in \mathrm{D}\left(\mathbb{C}^{dn}\right)$ *be the state of these registers. Suppose that for all permutation* $\pi \in S_n$ *it holds that* $\rho = \mathbf{W}_\pi \rho \mathbf{W}_\pi^*$*, where* $\mathbf{W}_\pi$ *permutes the contents of* $\mathsf{X}_1,\ldots,\mathsf{X}_n$ *according to* π*. Then for any choice of* $k \in \{2,3,\ldots,n-1\}$ *there exist a number* $N \in \mathbb{N}$*, a probability vector* $p \in \mathbb{R}^N$*, and a collection of density operators* $\{\sigma_i : i \in \{1,2,\ldots,N\}\} \subset \mathrm{D}\left(\mathbb{C}^d\right)$ *such that*

$$\left\| \rho^{\mathsf{X}_1\cdots\mathsf{X}_k} - \sum_{i=1}^{N} p_i \sigma_i^{\otimes k} \right\|_{\mathrm{Tr}} < \frac{4d^2k}{n}.$$

3 Proof of the Main Theorem

This section presents the detailed proof of the main theorem, using the results from the previous section.

Proof of Theorem 1.1. The inclusion $\mathsf{QMA} \subseteq \mathsf{QIP}_{\mathrm{short}}(O(\log n), c, s)$ is trivial, so we only need to prove $\mathsf{QIP}_{\mathrm{short}}(O(\log n), c, s) \subseteq \mathsf{QMA}$. Let $L \in \mathsf{QIP}_{\mathrm{short}}(m+1, c, s)$, where $m = O(\log n)$, and let V be the corresponding verifier. We will construct a verifier W for the QMA proof system. Because of Lemma 2.4, we can assume that any prover strategy in the first m rounds are unitary operators on $2m$ qubits, say $\mathbf{U}_1,\ldots,\mathbf{U}_m$. The constructed W expects to get as part of the proof, the classical descriptions of circuits $C_{\mathbf{U}_1,3^{-n}},\ldots,C_{\mathbf{U}_m,3^{-n}}$, i. e., the circuits that approximate the prover's operators with precision $1/3^n$. According to Corollary 2.7 the length of this proof is $O\left(m \cdot 5^{2m} \cdot \log^4\left(5^{2m} \cdot 3^n\right)\right) \in \mathsf{poly}(n)$. W uses this classical proof to simulate the first m rounds of the proof system, and produce the state of the whole system at the end of the mth round. This means the prover's and verifier's private spaces and the answer to the verifier from the mth round. We denote this state by $|\psi\rangle$. Using Corollary 2.8 and the fact that each circuit approximates the corresponding unitary with precision $1/3^n$, note that after applying $O(\log n)$-many of them, it is true that

$$\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_{\mathrm{Tr}} \leq \frac{m}{3^n} \leq \frac{1}{2^n},$$

for sufficiently large n; where $|\phi\rangle$ is the state of the whole system after the mth round in the case where the unitaries $\mathbf{U}_1,\ldots,\mathbf{U}_m$ were applied instead of the circuits.

We are left with specifying how W simulates the prover in the last, $(m+1)$th round. We use exactly the same method as was used in the proof of Theorem 2.3 in [2]. Our proof closely follows that proof as well. Since we are in the last round, we don't have to keep track of the prover's private space, so we can just describe its strategy as a quantum channel that transforms the private space of the prover with the question from the verifier to the answer to the verifier. Let's call this channel $\Phi \in \mathrm{C}(\mathcal{S},\mathcal{R})$ from now on; where $\mathcal{S}$ is the joint space associated to the prover's private space and the question, and $\mathcal{R}$ is the space associated to the answer. The input space $\mathcal{S}$ is on $q \stackrel{\mathrm{def}}{=} 2m+1 = O(\log n)$ qubits and the output space $\mathcal{R}$ is on $\mathsf{poly}(n)$ qubits. W expects to get $\rho_\Phi^{\otimes(N+k)}$ as the quantum part of its proof, where $\rho_\Phi \in \mathrm{D}(\mathcal{R}\otimes\mathcal{S})$ is the normalized Choi-Jamiołkowski representation of Φ, for N and k to be specified later. Let's divide up the quantum certificate given to W into registers R_1, S_1, R_2, S_2, …, R_{N+k}, S_{N+k}, where the space of each R_i is $\mathcal{R}$, and the space of each S_i is $\mathcal{S}$. W expects each $\mathsf{R}_i\mathsf{S}_i$ to contain a copy of ρ_Φ. To simulate the last round of the interactive proof system, W does the following.

1. Randomly permute the pairs $(\mathsf{R}_1,\mathsf{S}_1),\ldots,(\mathsf{R}_{N+k},\mathsf{S}_{N+k})$, according to a uniformly chosen permutation, and discard all but the first $(N+1)$ pairs.

2. Perform quantum state tomography on the registers $(\mathsf{S}_2,\ldots,\mathsf{S}_{N+1})$, and reject if the resulting approximation is not within trace-distance $\delta/2$ of the completely mixed state $(1/2^q)\,\mathbb{1}$, for δ to be specified below.

3. Simulate the channel specified by $(\mathsf{R}_1,\mathsf{S}_1)$ by post-selection. Reject if post-selection fails, otherwise simulate the last operation of V and accept if and only if V accepts.

Let $g(n)\in\mathsf{poly}(n)$ be such that $c(n)-s(n)\geq 1/g(n)$. We now set the parameters.

$$\varepsilon \stackrel{\text{def}}{=} \frac{1}{g\cdot 4^{q+1}},\qquad \delta \stackrel{\text{def}}{=} \frac{\varepsilon^2}{4},\qquad N \stackrel{\text{def}}{=} \left\lceil \frac{2^{10q}}{(\delta/2)^3}\right\rceil,\qquad k \stackrel{\text{def}}{=} \left\lceil \frac{(N+1)\cdot 4^{2q+1}}{\varepsilon}\right\rceil.$$

Note that $1/\varepsilon,1/\delta,N,k\in\mathsf{poly}(n)$.

Completeness. Suppose there exists a P that causes V to accept with probability $\geq c$. Let the certificate to W be the classical descriptions of circuits $C_{\mathbf{U}_1,3^{-n}},\ldots,C_{\mathbf{U}_m,3^{-n}}$, together with the state $\rho_\Phi^{\otimes(N+k)}$, where each $\mathsf{R}_i\mathsf{S}_i$ contains a copy of ρ_Φ, for $i\in\{1,2,\ldots,N+k\}$. After simulating the first m rounds, W produces $|\psi\rangle$ which is $\leq 1/2^n$ far from the correct $|\phi\rangle$ in the trace distance, just as described above. Note that in the simulation of the last round, step 1 doesn't change the state of registers $(\mathsf{R}_1,\mathsf{S}_1),\ldots,(\mathsf{R}_{N+1},\mathsf{S}_{N+1})$. According to Lemma 2.9, W rejects in step 2 with probability $\leq\delta/2$. In step 3, post-selection succeeds with probability $1/4^q$. If W was using $|\phi\rangle$ instead of $|\psi\rangle$ the probability of acceptance would be at least

$$\left(1-\frac{\delta}{2}\right)\frac{c}{4^q}.$$

So using $|\psi\rangle$, the probability that W accepts is at least

$$\left(1-\frac{\delta}{2}\right)\frac{c}{4^q}-\frac{1}{2^n}\geq\frac{c}{4^q}-\varepsilon-\frac{1}{2^n}.$$

Soundness. Suppose that all P causes V to accept with probability $\leq s$. Note that, without loss of generality any classical proof specifies some set of unitaries that correspond to a valid prover strategy. Hence it is still true, that after W simulates the first m rounds using the given circuits, it ends up with a state $|\psi\rangle$ that is at most $1/2^n$ far from a state $|\phi\rangle$, where $|\phi\rangle$ can be produced by some P interacting with V.

Now consider the situation that the state of $(\mathsf{S}_1,\ldots,\mathsf{S}_{N+1})$ before step 2 has the form

$$\sigma^{\otimes(N+1)}, \tag{3.1}$$

for some $\sigma\in\mathrm{D}(\mathcal{S})$. (The classical part of the proof has been used up and discarded before step 1.) We consider two cases:

- Suppose that $\|\sigma - (1/2^q)\,\mathbb{1}\|_{\mathrm{Tr}} < \delta$. Let the state of $(\mathsf{R}_1, \mathsf{S}_1)$ before step 3 be $\xi \in \mathrm{D}(\mathcal{R} \otimes \mathcal{S})$, so we have $\mathrm{Tr}_{\mathcal{R}}(\xi) = \sigma$. Because of the same argument as in [2], there exists a state $\tau \in \mathrm{D}(\mathcal{R} \otimes \mathcal{S})$ such that $\mathrm{Tr}_{\mathcal{R}}(\tau) = (1/2^q)\,\mathbb{1}$ and $\frac{1}{2}\|\tau - \xi\|_{\mathrm{Tr}} \leq \varepsilon$. Given this τ, the post-selection in step 3 succeeds with probability $1/4^q$, so the acceptance in step 3 occurs with probability at most $s/4^q + 1/2^n$. Given ξ instead of τ, W will accept with probability at most

$$\frac{s}{4^q} + \frac{1}{2^n} + \varepsilon.$$

- If $\|\sigma - (1/2^q)\,\mathbb{1}\|_{\mathrm{Tr}} \geq \delta$, then in step 2, W will accept with probability $\leq \delta/2$. (Here we used Lemma 2.9.)

Since $\delta/2 \leq s/4^q + 1/2^n + \varepsilon$ then in both cases acceptance occurs with probability $\leq s/4^q + 1/2^n + \varepsilon$.

Now suppose that the state of $(\mathsf{S}_1, \ldots, \mathsf{S}_{N+1})$ before step 2 has the form

$$\sum_i p_i \sigma_i^{\otimes(N+1)}, \tag{3.2}$$

for some probability vector p and some set $\{\sigma_i\} \subset \mathrm{D}(\mathcal{S})$. Since (3.2) is a convex combination of states of the form (3.1), acceptance will occur with probability $\leq s/4^q + 1/2^n + \varepsilon$. In the real scenario, by Theorem 2.10, it is true that the state of $(\mathsf{S}_1, \ldots, \mathsf{S}_{N+1})$ after step 1 will be ε close to a state of the form (3.2), in the trace distance. So the probability of acceptance of W will be $\leq s/4^q + 2\varepsilon + 1/2^n$. Since

$$\frac{c}{4^q} - \varepsilon - \frac{1}{2^n} - \left(\frac{s}{4^q} + 2\varepsilon + \frac{1}{2^n}\right) \geq \frac{1}{h(n)},$$

for some $h(n) \in \mathsf{poly}(n)$, it holds that $L \in \mathsf{QMA}$. □

4 An Open Problem

As a final remark, we mention an open problem that we think is interesting. Let us consider interactive proof systems which are similar to the ones studied in this paper but the polynomial-length message is at the beginning of the interaction, not at the end. More precisely, the interaction starts with a poly-length message from the prover and then continues with a conversation between the prover and the verifier, where the combined length of all messages is at most logarithmic. What is the power of this class?

Note that the power of this class doesn't change if we allow a logarithmic-length interaction both before and after the polynomial-length message. The reason is that in this case we can start the interaction with the prover sending the long message, along with the private space of the verifier. Then the verifier flips a coin and decides to continue the protocol forwards or backwards, and accepts if it ends up in the accepting state or initial state, respectively. This idea has appeared, for example, in [8].

Also note that this proof system is 'somewhere in between' BQP and QIP. If there is no long message from the prover (i. e., the length of the whole interaction is at most logarithmic), then the proof system has the same power as BQP [2]. On the other hand, if there are two polynomial-length messages from the prover then the proof system has the full power of QIP [10].

Acknowledgements

The author would like to thank Rahul Jain for helpful discussions on the topic, and anonymous referees for constructive comments on an earlier version of this paper.

References

[1] DORIT AHARONOV AND TOMER NAVEH: Quantum NP - a survey. 2002. [arXiv:quant-ph/0210077] 1, 3

[2] SALMAN BEIGI, PETER SHOR, AND JOHN WATROUS: Quantum interactive proofs with short messages. *Theory of Computing*, 7(1):101–117, 2011. [doi:10.4086/toc.2011.v007a007, arXiv:1004.0411] 2, 3, 4, 5, 6, 8

[3] HUGUE BLIER AND ALAIN TAPP: All languages in NP have very short quantum proofs. In *Third International Conference on Quantum, Nano and Micro Technologies*, pp. 34–37, 2009. [doi:10.1109/ICQNM.2009.21, arXiv:0709.0738] 1

[4] MATTHIAS CHRISTANDL, ROBERT KÖNIG, GRAEME MITCHISON, AND RENATO RENNER: One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007. [doi:10.1007/s00220-007-0189-3, arXiv:quant-ph/0602130] 6

[5] CHRISTOPHER M. DAWSON AND MICHAEL A. NIELSEN: The Solovay-Kitaev algorithm. *Quantum Information and Computation*, 6(1):81–95, January 2006. [arXiv:quant-ph/0505030] 5

[6] GUS GUTOSKI AND JOHN WATROUS: Toward a general theory of quantum games. In *Proceedings of the 39th annual ACM Symposium on Theory of Computing*, STOC '07, pp. 565–574, 2007. [doi:10.1145/1250790.1250873, arXiv:quant-ph/0611234] 5

[7] RAHUL JAIN, ZHENGFENG JI, SARVAGYA UPADHYAY, AND JOHN WATROUS: QIP = PSPACE. In *Proceedings of the 42nd annual ACM Symposium on Theory of Computing*, STOC '10, pp. 573–582, 2010. [doi:10.1145/1806689.1806768, arXiv:0907.4737] 1

[8] JULIA KEMPE, HIROTADA KOBAYASHI, KEIJI MATSUMOTO, AND THOMAS VIDICK: Using entanglement in quantum multi-prover interactive proofs. In *23rd Annual IEEE Conference on Computational Complexity*, pp. 211–222, June 2008. [doi:10.1109/CCC.2008.6, arXiv:0711.3715] 8

[9] A. YU KITAEV: Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997. [doi:10.1070/RM1997v052n06ABEH002155] 5

[10] ALEXEI KITAEV AND JOHN WATROUS: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd annual ACM Symposium on Theory of Computing*, STOC '00, pp. 608–617, 2000. [doi:10.1145/335305.335387] 1, 8

[11] HIROTADA KOBAYASHI AND KEIJI MATSUMOTO: Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003. [doi:10.1016/S0022-0000(03)00035-7, arXiv:cs/0102013] 5

[12] CARSTEN LUND, LANCE FORTNOW, HOWARD KARLOFF, AND NOAM NISAN: Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, October 1992. [doi:10.1145/146585.146605] 1

[13] CHRIS MARRIOTT AND JOHN WATROUS: Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. [doi:10.1007/s00037-005-0194-x, arXiv:cs/0506068] 2

[14] MICHAEL A. NIELSEN AND ISAAC L. CHUANG: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 3, 5

[15] ADI SHAMIR: IP = PSPACE. *J. ACM*, 39(4):869–877, October 1992. [doi:10.1145/146585.146609] 1

[16] JOHN WATROUS: PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003. [doi:10.1016/S0304-3975(01)00375-9] 1, 3

[17] JOHN WATROUS: Quantum computational complexity. April 2008. [arXiv:0804.3401] 3

[18] JOHN WATROUS: Theory of quantum information. Lecture notes from Fall 2008, `http://www.cs.uwaterloo.ca/~watrous/quant-info/`, 2008. 3, 6

AUTHOR

Attila Pereszlényi
Ph. D. student
Centre for Quantum Technologies, National University of Singapore, Singapore
attila.pereszlenyi@gmail.com