Using Entanglement in Quantum Multi-Prover Interactive Proofs

Julia Kempe*
School of Computer Science
Tel Aviv University
Tel Aviv, Israel

Hirotada Kobayashi†
Principles of Informatics Research Division
National Institute of Informatics
Tokyo, Japan

Keiji Matsumoto†
Principles of Informatics Research Division
National Institute of Informatics
Tokyo, Japan

Thomas Vidick‡
Computer Science Division
University of California, Berkeley
USA

Abstract

The central question in quantum multi-prover interactive proof systems is whether or not entanglement shared among provers affects the verification power of the proof system. We study for the first time positive *aspects of prior entanglement and show how it can be used to parallelize any multi-prover quantum interactive proof system to a* one-round *system with* perfect completeness*, soundness bounded away from* 1 *by an inverse polynomial in the input size, and one extra prover. Alternatively, we can also parallelize to a three-turn system with the same number of provers, where the verifier only broadcasts the outcome of a coin flip. This "public-coin" property is somewhat surprising, since in the classical case public-coin multi-prover interactive proofs are equivalent to single prover ones.*

1 Introduction

Multi-prover interactive proof systems are a central notion in theoretical computer science. An important generalization of interactive proof systems [13, 4], they were originally introduced in [6] in a cryptographic context. Later it was shown [5, 12] that the class MIP of languages having a multi-prover interactive proof system is equal to NEXP, which led to the development of the theory of inapproximability and probabilistically checkable proofs [10, 3, 2].

In a multi-prover interactive proof system, a verifier communicates with several provers, who do not communicate with each other. One of the central challenges in this area is to understand the power of *quantum* multi-prover interactive proof systems (QMIP systems). In particular, the major open question is how *entanglement* shared among the provers affects these systems. This question is unique to the quantum world, since the related classical resource of shared randomness is known not to affect the power of such systems. It is not even clear whether entanglement *increases* or *decreases* the verification power of QMIP systems. On one hand, using entanglement, dishonest provers might cheat more easily, thereby breaking the soundness of the system. On the other hand, the increased power that entanglement gives to honest provers could be harnessed by the verifier, increasing the expressivity of the proof system.

To the best of our knowledge, all previous results in this area (see below) have focused on the former case, studying the *negative* effects of entanglement, i.e., whether or not *dishonest* entangled provers can break proof systems that are sound for any dishonest *unentangled* provers. Our work is the first to focus on the *positive* aspects of entanglement, where shared entanglement may be advantageous to *honest* provers.

1.1 Previous and related work

Watrous [25] defined quantum interactive proof systems (QIP) with a *single* prover in analogy with classical single-prover interactive proofs, and proved that PSPACE had 3-message quantum interactive proofs. Kitaev and Wa-

*Work partly done while at LRI, Univ. de Paris-Sud, Orsay. Partially supported by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848, by an Alon Fellowship of the Israeli Higher Council of Academic Research and by a grant of the Israeli Science Foundation.

†Supported by the Strategic Information and Communications R&D Promotion Programme No. 031303020 of the Ministry of Internal Affairs and Communications of Japan and the Grant-in-Aid for Scientific Research (B) No. 18300002 of the Ministry of Education, Culture, Sports, Science and Technology of Japan.

‡Work partly done while at LRI, Univ. de Paris-Sud, Orsay and DI, École Normale Supérieure, Paris.

1093-0159/08 $25.00 © 2008 IEEE
DOI 10.1109/CCC.2008.6

trous [18] showed that these systems can be made perfect complete and can be parallelized to three turns. As such, some of our results can be seen as generalizations to the multi-prover case, and some of our proof techniques originate in that paper. Kitaev and Watrous also showed a parallel repetition theorem for QIP, which is currently not known to hold in the multi-prover case.

Kobayashi and Matsumoto [19] introduced QMIP systems with a quantum verifier, and proved that the class of languages having a quantum multi-prover interactive proof system is equal to NEXP when the provers do not share any prior entanglement, and is contained in NEXP when they share at most polynomially many entangled qubits. Cleve, Høyer, Toner, and Watrous [9] studied multi-prover interactive proof systems in which the verifier remains classical but provers may initially share entanglement, and presented several protocols for which shared EPR pairs can increase the power of dishonest provers. They also proved that the class of languages having some restricted version of multi-prover interactive proof system, denoted by $\oplus\mathrm{MIP}^*(2,1)$, is contained in EXP when provers are allowed to share prior entanglement (Wehner [27] improved the upper bound to $\mathrm{QIP}(2)$, the class of languages having a two-message quantum interactive proof system), which is in stark contrast to the corresponding class $\oplus\mathrm{MIP}(2,1)$ without prior entanglement, which is equal to NEXP. Very recently, Kempe, Kobayashi, Matsumoto, Toner, and Vidick [15] gave limits on the cheating power of dishonest entangled provers in some quantum and classical multi-prover interactive proof systems, by showing how such proof systems can be "immunized" against the use of entanglement by dishonest provers. Ito, Kobayashi, Preda, Sun, and Yao [14] and Cleve, Gavinsky, and Jain [8] also gave limits on the cheating power of entangled provers for some classical multi-prover interactive proof systems.

All these studies focus only on the *negative* aspects of prior entanglement, i.e., whether or not *dishonest* but prior-entangled provers can break the soundness of the proof system.

1.2 Our Results

This paper studies the *positive* aspects of prior entanglement and shows a number of general properties of QMIP systems, extensively using prior entanglement for *honest* provers. Our main theorem states that any quantum k-prover interactive proof system that may involve polynomially many rounds can be parallelized to a *one-round* quantum $(k+1)$-prover interactive proof system of *perfect* completeness and such that the gap between completeness and soundness accepting probabilities is still bounded by an inverse-polynomial.

To state our results more precisely, let $\mathrm{QMIP}(k,m,c,s)$ denote the class of languages having an m-turn quantum k-prover interactive proof system with completeness at least c and soundness at most s, where provers are allowed to share an arbitrary amount of entanglement. We call the difference $c-s$ the "gap" in this paper. As commonly used in classical multi-prover interactive proofs we use the term "round" to describe an interaction consisting of questions from the verifier followed by answers from the provers. We use the term "turn" for messages sent in one direction. One round consists of two turns: a turn for the verifier and a turn for the provers. Let poly and poly^{-1} be the sets of all functions upper-bounded by a polynomial and lower-bounded by an inverse polynomial in the input size, respectively. Throughout this paper we assume that the number m of turns and the number k of provers are functions in poly, and that completeness c and soundness s are functions of the input size $c,s\colon \mathbb{Z}^+ \to [0,1]$. We show the following main theorem.

Theorem 1. *For any $k,m \in \mathrm{poly}$ and c,s satisfying $c-s \in \mathrm{poly}^{-1}$ there exists a function $p \in \mathrm{poly}$ such that $\mathrm{QMIP}(k,m,c,s) \subseteq \mathrm{QMIP}\left(k+1,2,1,1-\frac{1}{p}\right)$.*

Since it is easy to amplify the success probability without increasing the number of rounds by running multiple instances of a proof system in parallel using a different set of provers for every instance, the above theorem shows that one-round (i.e., two-turn) QMIP systems are as powerful as general QMIP systems.

Corollary 2. *For any $k,m \in \mathrm{poly}$ and c,s satisfying $c-s \in \mathrm{poly}^{-1}$, and $p \in \mathrm{poly}$, there exists a $k' = O(k\,p\,m^2/(c-s)^2)$ such that $\mathrm{QMIP}(k,m,c,s) \subseteq \mathrm{QMIP}(k',2,1,2^{-p})$.*

The proof of our main theorem comes in three parts, corresponding to Sections 3, 4, and 5. The first part shows how to convert any QMIP system with two-sided bounded error into one with one-sided bounded error of perfect completeness without changing the number of provers. The second part shows that any QMIP system with polynomially many turns can be parallelized to one with only three turns in which the gap between completeness and soundness is still bounded by an inverse-polynomial. Again the number of provers remains the same in this transformation. Finally, the third part shows that any three-turn QMIP system with sufficiently large gap can be converted into a two-turn (i.e., one-round) QMIP system with inverse-polynomial gap, by adding an extra prover.

Similar statements to our first and second parts have already been shown by Kitaev and Watrous [18] for single-prover quantum interactive proofs. Their proofs, however, heavily rely on the fact that a single quantum prover can apply arbitrary operators over all the space except for the private space of the verifier. This is not the case any more for

quantum multi-prover interactive proofs, since now a quantum prover cannot access the qubits in the private spaces of the other quantum provers, in addition to those in the private space of the verifier. Hence new methods are required for the multi-prover case.

To transform proof systems so that they have perfect completeness, our basic idea is to adapt the quantum rewinding technique developed for quantum zero-knowledge proofs by Watrous [26] to our setting. We show how the main idea behind this technique can be used to "rewind" an unsuccessful computation that would result in rejection into a successful one. To this end, we first modify the proof system so that the honest provers can convince the verifier with probability exactly $\frac{1}{2}$ using some initial shared state and moreover no other initial shared state achieves a higher acceptance probability. This initial shared state corresponds to the auxiliary input in the case of quantum zero-knowledge proofs, and as in that scenario we can prove that the sequence of forward, backward, and forward executions of the protocol achieves perfect completeness. The obvious problem of this construction lies in proving soundness, as the dishonest provers may not use the same strategies for all of the three executions of the proof system. To settle this, we design a simple protocol that tests if the second backward execution is indeed a backward simulation of the first forward execution. The verifier performs with equal probability either the original rewinding protocol or this invertibility test without revealing which test the provers are undergoing. This forces the provers to use essentially the same strategies for the first two executions of the protocol, which is sufficient to bound the soundness. As a result we prove the following.

Theorem 3. *For any $k, m \in \mathrm{poly}$ and c, s satisfying $c - s \in \mathrm{poly}^{-1}$, and $p \in \mathrm{poly}$, there exists $m' \in \mathrm{poly}$ such that $\mathrm{QMIP}(k, m, c, s) \subseteq \mathrm{QMIP}(k, m', 1, 2^{-p})$.*

For the parallelization to three turns, our approach is to first show that any QMIP system with sufficiently large gap can be converted into another QMIP system with the same number of provers, in which the number of rounds (turns) becomes almost half of that in the original proof system. The proof idea is that the verifier in the first turn receives the snapshot state from the original system after (almost) half of turns have been executed, and then with equal probability executes either a forward-simulation or a backward-simulation of the original system from that turn on. Honest provers only have to simulate the original system to convince the verifier, while any strategy of dishonest provers with unallowable high success probability would lead to a strategy of dishonest provers in the original system that contradicts the soundness condition. By repeatedly applying this modification, together with Theorem 3 as preprocessing, we can convert any QMIP system into a three-turn QMIP system with the same number of provers that still has an inverse polynomial gap.

Theorem 4. *For any $k, m \in \mathrm{poly}$ and c, s satisfying $c - s \in \mathrm{poly}^{-1}$, there exists $p \in \mathrm{poly}$ such that $\mathrm{QMIP}(k, m, c, s) \subseteq \mathrm{QMIP}\left(k, 3, 1, 1 - \frac{1}{p}\right)$.*

For $k = 1$, this gives an alternative proof of the parallelization theorem due to Kitaev and Watrous [18] for single-prover quantum interactive proofs. It is interesting to note that our parallelization method does not need the controlled-swap test at all, while it *is* the key test in the Kitaev-Watrous parallelization method. Another point worth mentioning in our method is that, at every time step of our parallelized protocol, the whole system has only one snapshot state of the original system. This is in contrast to the fact that the whole system has to simultaneously treat many snapshot states in the Kitaev-Watrous method. The merit of our method is, thus, that we do not need to treat the possible entanglement among different snapshot states when analyzing soundness, which may be a main reason why our method works well even for the multi-prover case. Moreover, our method is more space-efficient than the Kitaev-Watrous method, in particular when we parallelize a system with polynomially many rounds.

To prove the third part, we will take a detour by proving that

(i) any three-turn QMIP system with sufficiently large gap can be modified to a three-turn *public-coin* QMIP system with the same number of provers and a gap of roughly similar order of magnitude,

(ii) any three-turn public-coin QMIP system can be converted into a two-turn QMIP system without changing completeness and soundness, by adding one extra prover.

The notion of public-coin QMIP systems we use is a natural generalization of public-coin quantum interactive proofs in the single-prover case introduced by Marriott and Watrous [20]. The corresponding complexity class is denoted by $\mathrm{QMIP}_{\mathrm{pub}}(k, m, c, s)$ in this paper. Intuitively, at every round, a public-coin quantum verifier flips a fair classical coin at most polynomially many times, and then simply broadcasts the result of these coin-flips to all the provers. Property (i) is a generalization of the result by Marriott and Watrous [20] to the multi-prover case, whereas property (ii) is completely new. The idea to prove (ii), assuming that the number of provers in the original proof system is k, is to send questions only to the first k provers in the new $(k+1)$-prover system, requesting the original second messages from the k provers in the original system. The verifier expects to receive from the $(k+1)$-st prover

the original first messages from the k provers in the original system without asking any question to that prover. The public-coin property of the original system implies the non-adaptiveness of the messages from the verifier, which is essential to prove (ii). In fact, there is a way to directly prove the third part, but our detour enables us to show another two important properties of QMIP systems. Specifically, property (i) essentially proves the equivalence of *public-coin* quantum k-prover interactive proofs and general quantum k-prover interactive proofs, for any k.

Theorem 5. *For any $k, m \in \mathrm{poly}$ and c, s satisfying $c - s \in \mathrm{poly}^{-1}$, and $p \in \mathrm{poly}$, there exists $m' \in \mathrm{poly}$ such that $\mathrm{QMIP}(k, m, c, s) \subseteq \mathrm{QMIP}_{\mathrm{pub}}(k, m', 1, 2^{-p})$.*

Note that in the classical case, public-coin multi-prover interactive proofs are only as powerful as single-prover interactive proofs: because every prover receives the same question from the verifier it means that every prover knows how other provers will behave and the joint strategy of the provers can therefore be simulated by a single prover. Hence, these systems cannot be as powerful as general classical multi-prover interactive proofs unless $\mathrm{NEXP} = \mathrm{PSPACE}$. In contrast, our result shows that in the quantum case, public-coin QMIP systems *are* as powerful as general QMIP systems. The non-triviality of public-coin QMIP systems may be explained as follows: even if every quantum prover knows how other quantum provers will behave, still each quantum prover can apply only local transformations over a part of some state that may be entangled among the provers, which is not enough to simulate every possible strategy a single quantum prover could follow.

Property (ii) for the case $k = 1$ implies that any language in QIP (and thus in PSPACE) has a *two-prover one-round* quantum interactive proof system of perfect completeness with exponentially small error in soundness, since any language in QIP has a three-message public-coin quantum interactive proof system of perfect completeness with exponentially small error in soundness [20].

Corollary 6. *For any $p \in \mathrm{poly}$, $\mathrm{QIP} \subseteq \mathrm{QMIP}(2, 2, 1, 2^{-p})$ (and thus $\mathrm{PSPACE} \subseteq \mathrm{QMIP}(2, 2, 1, 2^{-p})$).*

In the classical case a similar statement to the last corollary was shown by Cai, Condon, and Lipton [7] (and the stronger statement that two-prover one-round interactive proofs are as powerful as general multi-prover interactive proofs was shown later by Feige and Lovász [11]). All these results are, however, not known to hold under the existence of prior entanglement among the provers. Before our result, it has even been open if PSPACE has a two-prover one-round quantum interactive proof system. (Very recently, Kempe et al. [15] succeeded in proving that the classical two-prover one-round interactive proof system for PSPACE in Ref. [7] is sound in a weak sense against any pair of dishonest prior-entangled provers: soundness is bounded away from one by an inverse-polynomial. Their result is incomparable to ours since on one hand we have a much stronger soundness condition, and on the other both the verifier and the honest provers must be quantum. In contrast, in Ref. [15] both of them just follow a classical protocol.)

Finally, we stress again that our constructions extensively use the prior shared entanglement of the provers in a positive sense. In particular, even if the honest provers in the original proof system do not need any prior entanglement at all, the honest provers in the constructed proof system do need prior entanglement in many cases. Most of the properties proved in this paper (Theorems 1 and 5 and Corollary 6 in particular) are not known to hold when considering only initially unentangled honest provers, and thus give first evidence that sharing prior entanglement may be advantageous even to honest provers.

2 Preliminaries

We assume that the reader is familiar with the quantum formalism, including the quantum circuit model and definitions of mixed quantum states (density operators) and fidelity (all of which are discussed in detail in Refs. [22, 17], for instance). This section summarizes some of the notions and notations that are used in this paper, reviews the model of quantum multi-prover interactive proof systems and introduces the notion of *public-coin* quantum multi-prover interactive proof systems.

As in earlier work [25, 18, 19], we define QMIP systems in terms of quantum circuits. It is assumed that our circuits consist of unitary gates, which is sufficient since non-unitary and unitary quantum circuits are equivalent in computational power [1]. To avoid unnecessary complication, however, in the subsequent sections the descriptions of protocols often include non-unitary operations (measurements). Even in such cases, it is always possible to construct unitary quantum circuits that essentially achieve the same outcome. A notable exception is in the definition of the public-coin quantum verifier, where we want to define the public coin-flip to be a classical operation. This requires a non-unitary operation for the verifier, the (classical) public coin-flip.

When proving statements that involve the perfect-completeness property, we assume that our universal gate set satisfies some conditions, which may not hold with an arbitrary universal gate set. Specifically, we assume that the Hadamard transformation and any classical reversible transformations are exactly implementable in our gate set. Note that this condition is satisfied by most of the stan-

dard gate sets including the Shor basis [23] consisting of the Hadamard gate, the controlled-i-phase-shift gate, and the Toffoli gate, and thus, we believe that this condition is not restrictive. We stress that most of our main statements do hold with an arbitrary choice of universal gate set (the completeness and soundness conditions may become worse by negligible amounts in some of the claims, which does not affect the final main statements).

All Hilbert spaces in this paper are of dimension a power of two, spanned by qubits. We will use the following property of fidelity.

Lemma 7 ([24, 21])**.** *For any density operators ρ, σ, ξ over a Hilbert space $\mathcal{H}$, $F(\rho,\sigma)^2 + F(\sigma,\xi)^2 \leq 1 + F(\rho,\xi)$.*

Quantum Multi-Prover Interactive Proof Systems (QMIP systems): Throughout this paper k and k' denote the number of provers and m, m' denote the number of turns. All of these are from the set of polynomially bounded functions in the input size $|x|$, denoted by poly. Further, c and s denote functions of the input size into $[0,1]$ corresponding to completeness and soundness. For notational convenience in what follows we will omit the arguments of these functions.

A quantum k-prover interactive proof system consists of a verifier V with private quantum register V and k *provers* $P_1, \ldots, P_k$ with private quantum registers $\mathsf{P}_1, \ldots, \mathsf{P}_k$, as well as quantum message registers $\mathsf{M}_1, \ldots, \mathsf{M}_k$, which without loss of generality are assumed to have the same number of qubits, denoted by q_{M}. One of the private qubits of the verifier is designated as the *output qubit*. At the beginning of the protocol, all the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ are initialized to $|0\cdots 0\rangle$, and the qubits in $(\mathsf{P}_1, \ldots, \mathsf{P}_k)$ are in some *a priori shared state* $|\Phi\rangle$ prepared by the provers in advance (and hence possibly entangled), which without loss of generality can be assumed to be pure. No direct communication between the provers is allowed after that. The protocol consists of alternating turns of the provers and of the verifier, starting with the verifier, if m is even, and with the provers otherwise. At a turn of the verifier, V applies some polynomial-time circuit to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and then sends each register M_i to prover P_i. At a turn of the provers each prover P_i applies some transformation to the registers $(\mathsf{P}_i, \mathsf{M}_i)$ for $1 \leq i \leq k$ and sends M_i back to the verifier. The last turn is always a turn for the provers. After the last turn the verifier applies a polynomial-time circuit to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and then measures the output qubit in the standard basis, accepting if the outcome is $|1\rangle$ and rejecting otherwise.

Formally, an *m-turn polynomial-time quantum verifier* V for k-prover QMIP systems is a polynomial-time computable mapping from input strings x to a set of polynomial-time uniformly generated circuits $\{V^1, \ldots, V^{\lceil m+1/2 \rceil}\}$, and a partition of the space on which they act into registers $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, which consist of polynomially many qubits. Similarly an *m-turn quantum prover* P is a mapping from x to a set of circuits $\{P^1, \ldots, P^{\lceil m+1/2 \rceil}\}$ each acting on registers (P, M). No restrictions are placed on the complexity of this mapping or the size of P. We will denote the i-th prover, his registers and transformations with a subscript i. We will always assume that each prover P_i is *compatible* with the verifier, i.e. that the corresponding register M_i is the same for the verifier and the prover for $1 \leq i \leq k$.

The *protocol* $(V, P_1, \ldots, P_k, |\Phi\rangle)$ is the alternating application of prover's and verifier's circuits to the state $|0\cdots 0\rangle \otimes |\Phi\rangle$ in registers $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k, \mathsf{P}_1, \ldots, \mathsf{P}_k)$. For odd m, circuits $P_1^1 \otimes \cdots \otimes P_k^1$, V^1, $P_1^2 \otimes \cdots \otimes P_k^2$, V^2 and so on are applied in sequence terminating with $V^{m+1/2}$. If m is even, the sequence begins with V^1 followed by $P_1^1 \otimes \cdots \otimes P_k^1$ and so on up to $V^{m+2/2}$. We say that $(V, P_1, \ldots, P_k, |\Phi\rangle)$ accepts x if the designated output qubit in V is measured in $|1\rangle$ at the end of the protocol and call the probability with which this happens $p_{\mathrm{acc}}(x, V, P_1, \ldots, P_k, |\Phi\rangle)$.

Definition 8. A language L is in $\mathrm{QMIP}(k, m, c, s)$ iff there exists an m-turn polynomial-time quantum verifier V for quantum k-prover interactive proof systems such that, for every input x:

(Completeness) if $x \in L$, there exist m-turn quantum provers $P_1, \ldots, P_k$ and an a priori shared state $|\Phi\rangle$ such that $p_{\mathrm{acc}}(x, V, P_1, \ldots, P_k, |\Phi\rangle) \geq c$,

(Soundness) if $x \notin L$, for any m-turn quantum provers $P'_1, \ldots, P'_k$ and any a priori shared state $|\Phi'\rangle$, $p_{\mathrm{acc}}(x, V, P'_1, \ldots, P'_k, |\Phi'\rangle) \leq s$.

Next, we introduce the notions of *public-coin* quantum verifier and *public-coin* QMIP systems. These are natural generalizations of the corresponding notions in the single-prover case introduced by Marriott and Watrous [20]. Intuitively, a quantum verifier for quantum multi-prover interactive proof systems is public-coin if, at each of his turns, after receiving the message registers from the provers, he first flips a fair classical coin at most a polynomial number of times, and then simply broadcasts the result of these coin-flips to all the provers. No other messages are sent from the verifier to the provers. At the end of the protocol, the verifier applies some quantum operation to the messages received so far, and decides acceptance or rejection.

Formally, an m-turn polynomial-time quantum verifier for k-prover interactive proof systems is *public-coin* if each of the circuits $V^1, V^2, \ldots, V^{\lceil m-1/2 \rceil}$ implements the following procedure: V receives the message registers M_i from the provers, stores them in his private space, and then

flips a classical fair coin at most q_{M} times to generate a public string r_j, records r_j in his private space, and broadcasts r_j to all the provers. The circuit $V^{\lceil (m+1)/2 \rceil}$ is some unitary transformation controlled by all the recorded random strings r_j for $1 \leq j \leq \lceil (m-1)/2 \rceil$. A QMIP system is public-coin if the associated verifier is public-coin, and we define $\mathrm{QMIP}_{\mathrm{pub}}(k, m, c, s)$ to be the class of languages in $\mathrm{QMIP}(k, m, c, s)$ with a public-coin verifier.

3 QMIP with Perfect Completeness Equals General QMIP

In this section we prove Theorem 3, showing that any QMIP system with two-sided bounded error can be transformed into a one with one-sided bounded error of perfect completeness without changing the number of provers. For the case of a single prover, this was shown by Kitaev and Watrous [18], but their proof relies on the single prover performing a global unitary on the whole system, and therefore does not carry over to the multi-prover case (no prover has access to the other prover's private spaces and the private space of each prover might be arbitrarily large, so we cannot use the verifier to transfer those spaces from one prover to the other).

First, we introduce the notion of *perfectly rewindable* QMIP systems.

Definition 9. Let $s < \frac{1}{2}$. A language L has a perfectly rewindable m-turn quantum k-prover interactive proof system with soundness at most s iff there exists an m-turn polynomial-time quantum verifier V, such that, for every input x:

(Perfect Rewindability) if $x \in L$, there exists a set of m-turn quantum provers $P_1, \ldots, P_k$ such that $\max_{|\Phi\rangle} p_{\mathrm{acc}}(x, V, P_1, \ldots, P_k, |\Phi\rangle) = \frac{1}{2}$, where the maximum is taken over all a priori shared states $|\Phi\rangle$ prepared by $P_1, \ldots, P_k$.

(Soundness) if $x \notin L$, for any set of m-turn quantum provers $P'_1, \ldots, P'_k$ and any a priori shared state $|\Phi'\rangle$, $p_{\mathrm{acc}}(x, V, P'_1, \ldots, P'_k, |\Phi'\rangle) \leq s$.[1]

We first show how to modify any general QMIP system (with some appropriate conditions on completeness and soundness) to a perfectly rewindable one with the same k and m.

Lemma 10. *Let $c \geq \frac{1}{2} > s$. Then, any language L in $\mathrm{QMIP}(k, m, c, s)$ has a perfectly rewindable m-turn quantum k-prover interactive proof system with soundness at most s.*

[1] Note that both for completeness and soundness we first fix the provers' transformations and then maximize over all a priori shared states, which hence have a fixed dimension.

Proof. Let L be a language in $\mathrm{QMIP}(k, m, c, s)$ and V be the corresponding m-turn quantum verifier. We slightly modify V to construct another m-turn quantum verifier W for a perfectly rewindable proof system for L. The new verifier W, in addition to the registers of V, prepares another single-qubit register B, initialized to $|0\rangle$. For the first $m-2$ turns, W simply simulates V. In the $(m-1)$-st turn, a turn for the verifier, W proceeds like V would, but sends B to the first prover in addition to the qubits V would send in the original proof system. In the m-th turn the first prover is requested to send B back to W, in addition to the qubits sent to V in the original proof system. Then W proceeds for the final decision procedure like V would, but accepts iff V would have accepted *and* B is in the state $|1\rangle$. Notice that W accepts only if V would have accepted, so the soundness is obviously at most s in the constructed proof system.

For perfect rewindability we slightly modify the protocol for honest provers in the case $x \in L$. Let $|\Phi^*\rangle$ be the a priori shared state in the original proof system that maximizes the acceptance probability for the original honest provers and let $p_{\max}$ be that maximal acceptance probability. The new provers use $|\Phi^*\rangle$ as the a priori shared state and simulate the original provers except for the last turn. The only difference is that in the last turn the first prover proceeds as P_1 would, *and* applies a one-qubit unitary T to the qubit in B,

$$T : |0\rangle \to \sqrt{1 - \frac{1}{2p_{\max}}}|0\rangle + \sqrt{\frac{1}{2p_{\max}}}|1\rangle.$$

From the construction it is obvious that the maximum accepting probability is exactly equal to $\frac{1}{2}$ and that this maximum is achieved when the provers use the a priori shared state $|\Phi^*\rangle$. □

Now, we are ready to show the following lemma.

Lemma 11. *Let $c \geq \frac{1}{2}$ and $s < \frac{1}{25}$. Then,* $\mathrm{QMIP}(k, m, c, s) \subseteq \mathrm{QMIP}\left(k, 3m, 1, \frac{1}{2} + 2\sqrt{s} + \frac{5s}{2}\right)$.

Proof. The intuitive idea behind the proof of this lemma, using Watrous' "quantum rewinding technique", has already been explained in the introduction. We add some more intuition before proceeding to the technical proof. Using Lemma 10 we can assume that in the case of honest provers ($x \in L$) the acceptance probability with shared state $|\Phi^*\rangle$ is exactly $\frac{1}{2}$ and furthermore that no other a priori shared state achieves higher acceptance probability. The acceptance probability when the provers use any a priori shared state $|\Phi\rangle$ can be written as $p_{\mathrm{acc}} = \|\Pi_{\mathrm{acc}} Q |\Psi\rangle\|^2 = \|\Pi_{\mathrm{acc}} Q \Pi_{\mathrm{init}} |\Psi\rangle\|^2$, where $|\Psi\rangle = |0 \cdots 0\rangle_{(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)} \otimes |\Phi\rangle$, Q is the unitary transformation induced by the QMIP system just before the verifier's final measurement, Π_{init} is the projection on $|0 \cdots 0\rangle_{(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)}$ and Π_{acc} is the projection on $|1\rangle$ of the designated output qubit. In other words

the state $|\Psi^*\rangle = |0\cdots 0\rangle_{(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)} \otimes |\Phi^*\rangle$ maximizes the expression

$$\max_{|\Psi\rangle} \langle\Psi|\Pi_{\text{init}} Q^\dagger \Pi_{\text{acc}} Q \Pi_{\text{init}}|\Psi\rangle,$$

meaning that the matrix $M = \Pi_{\text{init}} Q^\dagger \Pi_{\text{acc}} Q \Pi_{\text{init}}$ has maximum eigenvalue $\frac{1}{2}$ with corresponding eigenvector $|\Psi^*\rangle$. Now we apply the quantum rewinding technique by performing forward, backward, and forward executions of the proof system in sequence. Perfect completeness follows from the fact that the initial state is an eigenvector of M with the corresponding eigenvalue exactly $\frac{1}{2}$, and the porof is similar to that of the zero-knowledge scenario of [26].

The challenge of this construction lies in the proof of soundness. If the input is a no-instance, the maximum eigenvalue of any matrix M corresponding to our proof system is small. This shows that if the dishonest provers are actually "not so dishonest", i.e., if they use the same strategies for all of the three (forward, backward, and forward) executions of the original proof system, the acceptance probability is still small. However, the problem arises when the dishonest provers change their strategies for some of the three executions. To settle this, we design a simple protocol that tests if the backward execution is indeed a backward simulation of the first forward execution. The verifier performs the original rewinding protocol or this invertibility test uniformly at random without revealing which test the provers are undergoing. Honest provers always pass this invertibility test, and thus perfect completeness is preserved. When the input is a no-instance, this forces the provers to use approximately the same strategies for the first two executions of the proof system, which is sufficient to bound the soundness.

We now proceed with the technical details. Let L be a language in $\text{QMIP}(k, m, c, s)$ and let V be the verifier in the perfectly rewindable m-turn quantum k-prover interactive proof system for L as per Lemma 10. We construct a $3m$-turn quantum verifier W of a new quantum k-prover interactive proof system for L. W has the same registers as V in the original proof system, and performs one of two tests, which we call "REWINDING TEST" and "INVERTIBILITY TEST". The exact protocol is described below, where for simplicity it is assumed that m is even (the case in which m is odd can be proved in a similar manner).

Verifier's Protocol for Perfect Completeness

1. Simulate the original verifier for the first m turns.
2. Choose $b \in \{0, 1\}$ uniformly at random. If $b = 0$, move to the REWINDING TEST described in Step 3, while if $b = 1$, move to the INVERTIBILITY TEST described in Step 4.
3. (REWINDING TEST)
   - 3.1. Apply $V^{\frac{m}{2}+1}$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Accept if the content of $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ corresponds to an accepting state in the original proof system. Otherwise apply $(V^{\frac{m}{2}+1})^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and send M_i to the ith prover, for $1 \le i \le k$.
   - 3.2. For $j = \frac{m}{2}$ down to 2, do the following: Receive M_i from the ith prover, for $1 \le i \le k$. Apply $(V^j)^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and send M_i to the ith prover, for $1 \le i \le k$.
   - 3.3. Receive M_i from the ith prover, for $1 \le i \le k$. Apply $(V^1)^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Perform a controlled-phase-flip: multiply the phase by -1 if all the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ are in state $|0\rangle$. Apply V^1 to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and send M_i to the ith prover, for $1 \le i \le k$.
   - 3.4. For $j = 2$ to $\frac{m}{2}$, do the following: Receive M_i from the ith prover, for $1 \le i \le k$. Apply V^j to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and send M_i to the ith prover, for $1 \le i \le k$.
   - 3.5. Receive M_i from the ith prover, for $1 \le i \le k$. Apply $V^{\frac{m}{2}+1}$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Accept if the content of $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ corresponds to an accepting state in the original proof system, and reject otherwise.
4. (INVERTIBILITY TEST)
   - 4.1. Send M_i to the ith prover, for $1 \le i \le k$.
   - 4.2. For $j = \frac{m}{2}$ down to 2, do the following: Receive M_i from the ith prover, for $1 \le i \le k$. Apply $(V^j)^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$, and send M_i to the ith prover, for $1 \le i \le k$.
   - 4.3. Receive M_i from the ith prover, for $1 \le i \le k$. Apply $(V^1)^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Accept if all the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ are in state $|0\rangle$, and reject otherwise.

Completeness: Assume the input x is in L. From the original provers $P_1, \ldots, P_k$ we design honest provers $R_1, \ldots, R_k$ for the constructed $3m$-turn system. Each new prover R_i has the same quantum register P_i as P_i has, and the new provers initially share $|\Phi^*\rangle$. For the first m turns each R_i simulates P_i. At the $(m + 2j)$-th turn for $1 \le j \le \frac{m}{2}$, R_i applies $(P_i^{\frac{m}{2}-j+1})^\dagger$ (i.e. the inverse of the $(m - 2j + 2)$-nd turn of the original P_i) . Finally, for the $(2m + 2j)$-th turn for $1 \le j \le \frac{m}{2}$, R_i again applies P_i^j.

It is obvious from this construction that the provers $R_1, \ldots, R_k$ can convince W with certainty when W performs the INVERTIBILITY TEST. We show that $R_1, \ldots, R_k$ can convince W with certainty even when W performs the

REWINDING TEST. In short, this holds for essentially the same reason that the quantum rewinding technique works well in the case of quantum zero-knowledge proofs, and we will closely follow that proof.

For notational convenience, let $\widetilde{P}^j = P_1^j \otimes \cdots \otimes P_k^j$ for $1 \leq j \leq \frac{m}{2}$, and let $Q = V^{\frac{m}{2}+1}\widetilde{P}^{\frac{m}{2}}V^{\frac{m}{2}} \cdots \widetilde{P}^1 V^1$. Recall that $M|\Psi^*\rangle = \frac{1}{2}|\Psi^*\rangle$ where $M = \Pi_{\text{init}}Q^\dagger\Pi_{\text{acc}}Q\Pi_{\text{init}}$. Define the unnormalized states $|\phi_0\rangle = \Pi_{\text{acc}}Q|\Psi^*\rangle$, $|\phi_1\rangle = \Pi_{\text{rej}}Q|\Psi^*\rangle$, $|\psi_0\rangle = \Pi_{\text{init}}Q^\dagger|\phi_0\rangle$, and $|\psi_1\rangle = \Pi_{\text{illegal}}Q^\dagger|\phi_0\rangle$ where $\Pi_{\text{illegal}} = I_{(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)} - \Pi_{\text{init}}$ is the projection onto states orthogonal to $|0\cdots0\rangle_{(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)}$ and $\Pi_{\text{rej}} = I_{(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)} - \Pi_{\text{acc}}$. Then, noticing that $|\Psi^*\rangle = \Pi_{\text{init}}|\Psi^*\rangle$, we have

$$\begin{aligned}|\psi_0\rangle &= \Pi_{\text{init}}Q^\dagger\Pi_{\text{acc}}Q|\Psi^*\rangle \\ &= \Pi_{\text{init}}Q^\dagger\Pi_{\text{acc}}Q\Pi_{\text{init}}|\Psi^*\rangle = M|\Psi^*\rangle = \frac{1}{2}|\Psi^*\rangle\end{aligned}$$

and thus,

$$\begin{aligned}Q^\dagger|\phi_1\rangle &= Q^\dagger\Pi_{\text{rej}}Q|\Psi^*\rangle = |\Psi^*\rangle - Q^\dagger\Pi_{\text{acc}}Q|\Psi^*\rangle \\ &= |\Psi^*\rangle - Q^\dagger|\phi_0\rangle = |\psi_0\rangle - |\psi_1\rangle.\end{aligned}$$

Hence, the state just before the controlled-phase-flip in Step 3.3 when entering the REWINDING TEST is exactly

$$\frac{1}{\||\phi_1\rangle\|}Q^\dagger|\phi_1\rangle = \frac{1}{\||\phi_1\rangle\|}(|\psi_0\rangle - |\psi_1\rangle).$$

Since $\Pi_{\text{init}}|\psi_0\rangle = |\psi_0\rangle$ and $\Pi_{\text{init}}|\psi_1\rangle = 0$, the controlled-phase-flip changes the state to

$$-\frac{1}{\||\phi_1\rangle\|}(|\psi_0\rangle + |\psi_1\rangle) = -\frac{1}{\||\phi_1\rangle\|}Q^\dagger|\phi_0\rangle.$$

Therefore, the state just after $V^{\frac{m}{2}+1}$ is applied in Step 3.5 is exactly

$$-\frac{1}{\||\phi_1\rangle\|}QQ^\dagger|\phi_0\rangle = -\frac{1}{\||\phi_1\rangle\|}|\phi_0\rangle,$$

and thus, the fact that $\Pi_{\text{acc}}|\phi_0\rangle = |\phi_0\rangle$ implies that the verifier W always accepts in Step 3.5.

Soundness: Now suppose that the input x is not in L. Let $R'_1, \ldots, R'_k$ be any k provers for the constructed $3m$-turn proof system, and let $|\psi\rangle$ be any a priori shared state. Let R_i^j be the transformation that R'_i applies at his $2j$-th turn, for $1 \leq i \leq k$ and $1 \leq j \leq \frac{3m}{2}$ and let Z denote the controlled-phase-flip operator in Step 3.3. Call $\widetilde{R}^j = R_1^j \otimes \cdots \otimes R_k^j$ for $1 \leq t \leq \frac{3m}{2}$, and define

$$\begin{aligned}U_1 &= \widetilde{R}^{\frac{m}{2}}V^{\frac{m}{2}} \cdots \widetilde{R}^2V^2\widetilde{R}^1V^1, \\ U_2 &= (V^1)^\dagger\widetilde{R}^m \cdots (V^{\frac{m}{2}-1})^\dagger\widetilde{R}^{\frac{m}{2}+2}(V^{\frac{m}{2}})^\dagger\widetilde{R}^{\frac{m}{2}+1}, \\ U_3 &= \widetilde{R}^{\frac{3m}{2}}V^{\frac{m}{2}} \cdots \widetilde{R}^{m+2}V^2\widetilde{R}^{m+1}V^1.\end{aligned}$$

There are three cases of acceptance in the constructed proof system. In the first case, the verifier W performs the REWINDING TEST and accepts in Step 3.1. This happens with probability $\frac{p_1}{2}$, where

$$p_1 = \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_1|\psi\rangle\|^2.$$

In the second case, the verifier W performs the REWINDING TEST and accepts in Step 3.5. This happens with probability $\frac{p_2}{2}$, where

$$p_2 = \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3ZU_2(V^{\frac{m}{2}+1})^\dagger\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle\|^2.$$

Finally, in the third case, the verifier W performs the INVERTIBILITY TEST and accepts in Step 4.3. This happens with probability $\frac{p_3}{2}$, where

$$p_3 = \|\Pi_{\text{init}}U_2U_1|\psi\rangle\|^2.$$

Hence, the total probability p_{acc} that W accepts x when communicating with $R'_1, \ldots, R'_k$ is given by $p_{\text{acc}} = \frac{1}{2}(p_1 + p_2 + p_3)$. From the soundness condition of the original proof system, it is obvious that $p_1 \leq s$. We shall show that $p_2 \leq 1 + 4\sqrt{s} + 4s - p_3$. This implies that $p_{\text{acc}} \leq \frac{1}{2} + 2\sqrt{s} + \frac{5s}{2}$, and the soundness condition follows.

Using the triangle inequality, we have that

$$\begin{aligned}&\|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3ZU_2(V^{\frac{m}{2}+1})^\dagger\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle\| \\ &\quad\leq \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3ZU_2(V^{\frac{m}{2}+1})^\dagger\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle \\ &\qquad - \Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3ZU_2U_1|\psi\rangle\| \\ &\qquad + \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3ZU_2U_1|\psi\rangle \\ &\qquad - \Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3Z\Pi_{\text{init}}U_2U_1|\psi\rangle\| \\ &\qquad + \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3Z\Pi_{\text{init}}U_2U_1|\psi\rangle\|.\end{aligned} \tag{1}$$

The first term (a) of the right-hand side of inequality (1) can be bounded from above as follows:

$$\begin{aligned}(a) \;&\leq \|V^{\frac{m}{2}+1}U_3ZU_2(V^{\frac{m}{2}+1})^\dagger\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle \\ &\qquad - V^{\frac{m}{2}+1}U_3ZU_2U_1|\psi\rangle\| \\ &= \|(V^{\frac{m}{2}+1})^\dagger\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle - U_1|\psi\rangle\| \\ &= \|\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle - V^{\frac{m}{2}+1}U_1|\psi\rangle\| \\ &= \| - \Pi_{\text{acc}}V^{\frac{m}{2}+1}U_1|\psi\rangle\| \\ &= \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_1|\psi\rangle\| = \sqrt{p_1} \leq \sqrt{s}.\end{aligned}$$

The second term (b) of the right-hand side of inequality (1) can be bounded from above as follows:

$$\begin{aligned}(b) \;&\leq \|V^{\frac{m}{2}+1}U_3ZU_2U_1|\psi\rangle - V^{\frac{m}{2}+1}U_3Z\Pi_{\text{init}}U_2U_1|\psi\rangle\| \\ &= \|U_2U_1|\psi\rangle - \Pi_{\text{init}}U_2U_1|\psi\rangle\| \\ &= \|\Pi_{\text{illegal}}U_2U_1|\psi\rangle\| = \sqrt{1 - p_3}.\end{aligned}$$

Here the last equality follows from the facts that $U_2U_1|\psi\rangle = \Pi_{\text{init}}U_2U_1|\psi\rangle + \Pi_{\text{illegal}}U_2U_1|\psi\rangle$ is a unit vector, that $\Pi_{\text{init}}U_2U_1|\psi\rangle$ and $\Pi_{\text{illegal}}U_2U_1|\psi\rangle$ are orthogonal, and that $\|\Pi_{\text{init}}U_2U_1|\psi\rangle\|^2 = p_3$.

Finally, since $\Pi_{\text{init}}U_2U_1|\psi\rangle$ is an unnormalized state parallel to some legal initial state and $Z\Pi_{\text{init}} = -\Pi_{\text{init}}$ from the definitions of Z and Π_{init}, the third term (c) of the right-hand side of inequality (1) can be bounded as follows by using the soundness condition of the original proof system:

$$\begin{aligned}(c) &= \| - \Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3\Pi_{\text{init}}U_2U_1|\psi\rangle\| \\ &= \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3\Pi_{\text{init}}U_2U_1|\psi\rangle\| \leq \sqrt{s}\end{aligned}$$

Putting everything together, we have

$$\begin{aligned}p_2 &= \|\Pi_{\text{acc}}V^{\frac{m}{2}+1}U_3ZU_2(V^{\frac{m}{2}+1})^\dagger\Pi_{\text{rej}}V^{\frac{m}{2}+1}U_1|\psi\rangle\|^2 \\ &\leq (2\sqrt{s} + \sqrt{1-p_3})^2 = 1 + 4\sqrt{s(1-p_3)} + 4s - p_3 \\ &\leq 1 + 4\sqrt{s} + 4s - p_3,\end{aligned}$$

as desired. □

To finish the proof of Theorem 3 it suffices to repeat sequentially the proof system obtained in Lemma 11 an appropriate number of times (and accept if and only if all the original verifiers would have accepted every time). To see that this reduces soundness exponentially with the number of repetitions, imagine by contradiction that there exists a set of provers that succeeds in the k-th repetition of the protocol with probability s' greater than the original protocol's soundness s. Then we can construct provers for the original protocol by letting them initially share the state of the provers at the end of the $k-1$-st repetition of the new protocol. These provers would be accepted with probability $s' > s$, a contradiction.

4 Parallelizing to Three Turns

In this section we prove Theorem 4, which reduces the number of turns to three without changing the number of provers. This is done by repeatedly converting any (2^l+1)-turn QMIP system into a $(2^{l-1}+1)$-turn QMIP system where the gap decreases, but is still bounded by an inverse-polynomial. We first show the following lemma.

Lemma 12. *Let $c^2 > s$. Then,* $\text{QMIP}(k, 4m+1, c, s) \subseteq \text{QMIP}\left(k, 2m+1, \frac{1+c}{2}, \frac{1+\sqrt{s}}{2}\right)$.

Proof. Let L be a language in $\text{QMIP}(k, 4m+1, c, s)$ and let V be the corresponding $(4m+1)$-turn quantum verifier. We construct a $(2m+1)$-turn quantum verifier W for the new quantum k-prover interactive proof system for L. The idea is that W first receives the snapshot state that V would have in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ just after the $(2m+1)$-st turn of the original system. W then executes with equal probability either a forward-simulation of the original system from the $(2m+1)$-st turn or a backward-simulation of the original system from the $(2m+1)$-st turn. In the former case, W accepts if and only if the simulation results in acceptance in the original proof system, while in the latter case W accepts if and only if the qubits in V are in state $|0\cdots0\rangle$.[2] Here is a detailed description of the protocol:

Verifier's Protocol to Half the Number of Turns

1. Receive V and M_1 from the first prover and M_i from the ith prover for $2 \leq i \leq k$.
2. Choose $b \in \{0, 1\}$ uniformly at random.
3. If $b = 0$, execute a forward-simulation of the original proof system as follows:
   - 3.1. Apply V^{m+1} to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Send b and M_i to the ith prover, for $1 \leq i \leq k$.
   - 3.2. For $j = m+2$ to $2m$, do the following: Receive M_i from the ith prover, for $1 \leq i \leq k$. Apply V^j to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Send M_i to the ith prover, for $1 \leq i \leq k$.
   - 3.3. Receive M_i from the ith prover, for $1 \leq i \leq k$. Apply V^{2m+1} to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Accept if the content of $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$ is an accepting state of the original proof system, and reject otherwise.
4. If $b = 1$, execute a backward-simulation of the original proof system as follows:
   - 4.1. Send b and M_i to the ith prover, for $1 \leq i \leq k$.
   - 4.2. For $j = m$ down to 2, do the following: Receive M_i from the ith prover, for $1 \leq i \leq k$. Apply $(V^j)^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Send M_i to the ith prover, for $1 \leq i \leq k$.
   - 4.3. Receive M_i from the ith prover, for $1 \leq i \leq k$. Apply $(V^1)^\dagger$ to the qubits in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k)$. Accept if the qubits in V are in state $|0\cdots0\rangle$, and reject otherwise.

Completeness: Assume the input x is in L. Let $P_1, \ldots, P_k$ be the honest quantum provers in the original proof system with a priori shared state $|\Phi\rangle$. Let $|\psi_{2m+1}\rangle$ be the quantum state in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k, \mathsf{P}_1, \ldots, \mathsf{P}_k)$ just after the $(2m+1)$-st turn in the original proof system. We construct honest provers $R_1, \ldots, R_k$ for the new $(2m+1)$-turn system. In addition to V and M_1, R_1 prepares P_1 in his private space. Similarly, in addition to M_i, R_i prepares

[2] Recall that in the original proof system the first turn was done by the provers, hence we do not measure the qubits in each M_i here.

P_i in his private space for $2 \leq i \leq k$. $R_1, \ldots, R_k$ initially share $|\psi_{2m+1}\rangle$ in $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k, \mathsf{P}_1, \ldots, \mathsf{P}_k)$. At the first turn of the constructed proof system, R_1 sends V and M_1 to W, while each R_i, for $2 \leq i \leq k$, sends M_i to W. At the $(2j-1)$-st turn for $2 \leq j \leq m+1$, if $b=0$, each R_i applies P_i^{m+j} (i.e. P_i's transformation at the $(2m+2j-1)$-st turn in the original system) while if $b=1$, each R_i applies $(P_i^{m-j+3})^\dagger$ (i.e. the inverse of P_i's transformation at the $(2m-2j+5)$-th turn in the original system) to the qubits in $(\mathsf{P}_i, \mathsf{M}_i)$, for $1 \leq i \leq k$. The provers $R_1, \ldots, R_k$ can then clearly convince W with probability at least c if $b=0$, and with certainty if $b=1$. Hence, W accepts every input $x \in L$ with probability at least $\frac{1+c}{2}$.

Soundness: Now suppose that x is not in L. Let $R'_1, \ldots, R'_k$ be arbitrary provers for the constructed proof system, and let $|\psi\rangle$ be an arbitrary quantum state that represents the state just after the first turn in the constructed system. Suppose that, at the $(2j-1)$-st turn for $2 \leq j \leq m+1$, each R'_i applies X_i^j if $b=0$ and Y_i^j if $b=1$, for $1 \leq i \leq k$ and write $\widetilde{X}^j = X_1^j \otimes \cdots \otimes X_k^j$ and $\widetilde{Y}^j = Y_1^j \otimes \cdots \otimes Y_k^j$. Define unitary transformations U_0 and U_1 by $U_0 = V^{2m+1}\widetilde{X}^{m+1}V^{2m}\cdots\widetilde{X}^2V^{m+1}$ and $U_1 = (V^1)^\dagger\widetilde{Y}^{m+1}\cdots(V^m)^\dagger\widetilde{Y}^2$, and let $|\alpha\rangle = \frac{1}{\|\Pi_{\mathrm{acc}}U_0|\psi\rangle\|}\Pi_{\mathrm{acc}}U_0|\psi\rangle$ and $|\beta\rangle = \frac{1}{\|\Pi_{\mathrm{init}}U_1|\psi\rangle\|}\Pi_{\mathrm{init}}U_1|\psi\rangle$, where Π_{acc} is the projection onto accepting states in the original proof system and Π_{init} is the projection on $|0\cdots0\rangle_{\mathsf{V}}$ in V. Then

$$\begin{aligned}\|\Pi_{\mathrm{acc}}U_0|\psi\rangle\| &= \frac{1}{\|\Pi_{\mathrm{acc}}U_0|\psi\rangle\|}\big|\langle\psi|U_0^\dagger\Pi_{\mathrm{acc}}U_0|\psi\rangle\big| \\ &= F\big(|\alpha\rangle\langle\alpha|, U_0|\psi\rangle\langle\psi|U_0^\dagger\big) \\ &= F\big(U_0^\dagger|\alpha\rangle\langle\alpha|U_0, |\psi\rangle\langle\psi|\big)\end{aligned}$$

and thus, the probability p_0 of acceptance when $b=0$ is given by $p_0 = F\big(U_0^\dagger|\alpha\rangle\langle\alpha|U_0, |\psi\rangle\langle\psi|\big)^2$. Similarly, the probability p_1 of acceptance when $b=1$ is given by $p_1 = F\big(U_1^\dagger|\beta\rangle\langle\beta|U_1, |\psi\rangle\langle\psi|\big)^2$. Hence the probability p_{acc} that W accepts x when communicating with $R'_1, \ldots, R'_k$ is given by

$$\begin{aligned}p_{\mathrm{acc}} = \frac{1}{2}(p_0+p_1) = \frac{1}{2}\Big(&F\big(U_0^\dagger|\alpha\rangle\langle\alpha|U_0, |\psi\rangle\langle\psi|\big)^2 \\ &+ F\big(U_1^\dagger|\beta\rangle\langle\beta|U_1, |\psi\rangle\langle\psi|\big)^2\Big)\end{aligned}$$

Therefore, from Lemma 7, we have

$$\begin{aligned}p_{\mathrm{acc}} &\leq \frac{1}{2}\Big(1 + F\big(U_0^\dagger|\alpha\rangle\langle\alpha|U_0, U_1^\dagger|\beta\rangle\langle\beta|U_1\big)\Big) \\ &= \frac{1}{2}\Big(1 + F\big(|\alpha\rangle\langle\alpha|, U_0U_1^\dagger|\beta\rangle\langle\beta|U_1U_0^\dagger\big)\Big)\end{aligned}$$

Note that $\Pi_{\mathrm{init}}|\beta\rangle = |\beta\rangle$ and thus $|\beta\rangle$ is a legal quantum state which could appear in the original proof system just after the first turn. Hence, from the soundness property of the original proof system,

$$\begin{aligned}\big\|\Pi_{\mathrm{acc}}U_0U_1^\dagger|\beta\rangle\big\|^2 = \big\|\Pi_{\mathrm{acc}}&V^{2m+1}\widetilde{X}^{m+1}V^{2m}\cdots \\ &\cdots\widetilde{X}^2V^{m+1}(\widetilde{Y}^2)^\dagger V^m\cdots(\widetilde{Y}^{m+1})^\dagger V^1|\beta\rangle\big\|^2 \leq s\end{aligned}$$

since V^1, $(\widetilde{Y}^{m+1})^\dagger, \cdots, V^m$, $(\widetilde{Y}^2)^\dagger$, V^{m+1}, $\widetilde{X}^2, \cdots, V^{2m}$, $\widetilde{X}^{m+1}, V^{2m+1}$ form a legal sequence of transformations in the original proof system.

Now, from the fact that $\Pi_{\mathrm{acc}}|\alpha\rangle = |\alpha\rangle$, we have

$$\begin{aligned}&F\big(|\alpha\rangle\langle\alpha|, U_0U_1^\dagger|\beta\rangle\langle\beta|U_1U_0^\dagger\big) \\ &\quad= \big|\langle\alpha|U_0U_1^\dagger|\beta\rangle\big| = \big|\langle\alpha|\Pi_{\mathrm{acc}}U_0U_1^\dagger|\beta\rangle\big| \\ &\quad\leq \|\Pi_{\mathrm{acc}}U_0U_1^\dagger|\beta\rangle\| \leq \sqrt{s}.\end{aligned}$$

Hence the probability p_{acc} that W accepts x is bounded by $p_{\mathrm{acc}} \leq \frac{1}{2} + \frac{\sqrt{s}}{2}$, which completes the proof. □

Now, by repeatedly applying the construction in the proof of Lemma 12, we can reduce the number of turns to three. The proof is straightforward, but we need to carefully keep track of the efficiency of the constructed verifiers in each application, since the construction is sequentially applied a logarithmic number of times.

Lemma 13. *For any $m \geq 4$ and any c, s such that $\varepsilon = 1-c$ and $\delta = 1-s$ satisfy $\delta > 2(m-1)\varepsilon$, $\mathrm{QMIP}(k, m, 1-\varepsilon, 1-\delta) \subseteq \mathrm{QMIP}\,(k, 3, 1-\varepsilon', 1-\delta')$, where $\varepsilon' = \frac{2\varepsilon}{m-1}$ and $\delta' = \frac{\delta}{(m-1)^2}$.*

Proof. Let l be such that $2^l + 1 \leq m \leq 2^{l+1}+1$. Trivially, $\mathrm{QMIP}(k, m, c, s) \subseteq \mathrm{QMIP}(k, 2^{l+1}+1, c, s)$. We show $\mathrm{QMIP}(k, 2^{l+1}+1, 1-\varepsilon, 1-\delta) \subseteq \mathrm{QMIP}(k, 3, 1-\frac{2\varepsilon}{m-1}, 1-\frac{\delta}{(m-1)^2})$.

Let L be a language in $\mathrm{QMIP}(k, 2^{l+1}+1, 1-\varepsilon, 1-\delta)$ and let $V^{(0)}$ be the corresponding $(2^{l+1}+1)$-turn quantum verifier. Given a description of $V^{(0)}$ one can compute in polynomial time a description of a (2^l+1)-turn quantum verifier $V^{(1)}$ following the proof of Lemma 12. The resulting proof system has completeness at least $1-\frac{\varepsilon}{2}$ and soundness at most $\frac{1}{2} + \frac{\sqrt{1-\delta}}{2} \leq 1 - \frac{\delta}{4}$. Crucially, the description of $V^{(1)}$ is at most some constant times the size of the description of $V^{(0)}$ plus an amount bounded by a polynomial in $|x|$. Hence it is obvious that, given a description of $V^{(0)}$, one can compute in polynomial time a description of a three-turn quantum verifier $V^{(l)}$ by repeatedly applying the construction in the proof of Lemma 12 l times. The resulting proof system has completeness at least $1 - \frac{\varepsilon}{2^l} \geq 1 - \frac{2\varepsilon}{m-1}$ and soundness at most $1 - \frac{\delta}{4^l} \leq 1 - \frac{\delta}{(m-1)^2}$, as desired. □

Theorem 4 now follows immediately from Theorem 3 and Lemma 13: For every $p \in \mathrm{poly}$ there is an $m' \in$

poly such that $\mathrm{QMIP}(k,m,c,s) \subseteq \mathrm{QMIP}(k,m',1,2^{-p}) \subseteq \mathrm{QMIP}\left(k,3,1,1-\frac{1-2^{-p}}{(m'-1)^2}\right)$. Now it suffices to observe that $\frac{1-2^{-p}}{(m'-1)^2} \in \mathrm{poly}^{-1}$.

5 Public-Coin Systems

In this section we present the last part to complete the proof of Theorem 1. We show how any three-turn QMIP system with sufficiently large gap can be converted into a two-turn QMIP system with one extra prover, in which the gap is bounded by an inverse-polynomial. Although it is also possible to give a direct proof of this fact, we will take a detour by showing how (i) any three-turn QMIP system with sufficiently large gap can be modified to a three-turn *public-coin* QMIP system with inverse-polynomial gap without changing the number of provers, and (ii) any three-turn public-coin QMIP system can be converted into a two-turn QMIP system without changing completeness and soundness, by adding an extra prover. The added benefits of our detour are a proof of the equivalence of public-coin QMIP systems and general QMIP systems (Theorem 5) and a proof that QIP and hence PSPACE has a two-prover one-round quantum interactive proof system of perfect completeness and exponentially small soundness (Corollary 6).

5.1 Converting to Public-Coin Systems

In this subsection we prove Theorem 5 showing that any language that has a quantum k-prover interactive proof system with two-sided bounded error also has a *public-coin* quantum k-prover interactive proof system of perfect completeness and exponentially small soundness.

We first show that any three-turn QMIP system with sufficiently large gap can be modified to a three-turn public-coin QMIP system with the same number of provers and inverse-polynomial gap. In the single-prover case, Marriott and Watrous [20] proved a similar statement. Our proof is a generalization of their proof (Theorem 5.4 in Ref. [20]) to the multi-prover case.

Lemma 14. *For any c, s satisfying $c^2 > s$, $\mathrm{QMIP}(k,3,c,s) \subseteq \mathrm{QMIP}_{\mathrm{pub}}(k,3,\frac{1+c}{2},\frac{1+\sqrt{s}}{2})$. Moreover, the message from the verifier to each prover in the public-coin system consists of only one classical bit.*

Proof. Let L be a language in $\mathrm{QMIP}(k,3,c,s)$ and let V be the corresponding three-turn quantum verifier. We construct a new verifier W for the public-coin system. The idea is that in the first turn W receives the reduced state in the original register V of the snapshot state just after the second turn (i.e., just after the first transformation of V) in the original proof system. W then flips a fair classical coin $b \in \{0,1\}$ and broadcasts b to the provers. At the third turn the ith prover is requested to send the register M_i of the original proof system, for $1 \leq i \leq k$. If $b = 0$ the qubits in $(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)$ should form the quantum state the original verifier V would possess just after the third turn of the original proof system. Now W applies V^2 to the qubits in $(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)$ and accepts if and only if the content of $(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)$ is an accepting state of the original proof system. On the other hand, if $b = 1$, the qubits in $(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)$ should form the quantum state the original verifier V would possess just after the second turn of the original proof system. Now W applies $(V^1)^\dagger$ to the qubits in $(\mathsf{V},\mathsf{M}_1,\ldots,\mathsf{M}_k)$ and accepts if and only if all the qubits in V are in state $|0\rangle$. The analysis of completeness and soundness of the constructed proof system is nearly identical to the one in Lemma 12, and is relegated to the full version of this paper [16]. □

Theorem 5 now follows directly from Theorem 4 and Lemma 14 together with sequential repetition: Theorem 4 and Lemma 14 imply that there is a $p' \in \mathrm{poly}$ such that

$$\begin{aligned}\mathrm{QMIP}(k,m,c,s) &\subseteq \mathrm{QMIP}\big(k,3,1,1-\frac{1}{p'}\big)\\ &\subseteq \mathrm{QMIP}_{\mathrm{pub}}\big(k,3,1,1-\frac{1}{4p'}\big)\end{aligned}$$

since $\frac{1}{2}\left(1+\sqrt{1-\frac{1}{p'}}\right) \leq 1-\frac{1}{4p'}$. Finally, sequential repetition gives that for all $p \in \mathrm{poly}$ there exists an $m' \in \mathrm{poly}$ such that $\mathrm{QMIP}_{\mathrm{pub}}\big(k,3,1,1-\frac{1}{4p'}\big) \subseteq \mathrm{QMIP}_{\mathrm{pub}}(k,m',1,2^{-p})$.

5.2 Parallelizing to Two Turns

Finally, we prove the last piece of Theorem 1 by showing that any three-turn public-coin quantum k-prover interactive proof system can be converted into a two-turn (i.e., one-round) $(k+1)$-prover system without changing completeness and soundness. The idea of the proof is to send questions only to the first k provers to request the original second messages from the k provers in the original system and to receive from the $(k+1)$-st prover the original first messages of the k provers in the original system without asking him any question.

Lemma 15. $\mathrm{QMIP}_{\mathrm{pub}}(k,3,c,s) \subseteq \mathrm{QMIP}(k+1,2,c,s)$.

Proof. Let L be a language in $\mathrm{QMIP}_{\mathrm{pub}}(k,m,c,s)$ and let V be the corresponding verifier.

The protocol can be viewed as follows: At the first turn, V first receives a quantum register M_i from the ith prover, for each $1 \leq i \leq k$. V flips a fair classical coin q_{M} times to generate a random string r of length q_{M}, and broadcasts r to all the provers. V also stores r in a quantum

register Q in his private space. Finally, at the third turn, V receives a quantum register N_i from the ith prover, for each $1 \leq i \leq k$. V then prepares a quantum register V for his work space, where all the qubits in V are initialized to state $|0\rangle$, applies the transformation V^{final} to the qubits in $(\mathsf{Q}, \mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_k, \mathsf{N}_1, \ldots, \mathsf{N}_k)$, and performs the measurement $\Pi = \{\Pi_{\text{acc}}, \Pi_{\text{rej}}\}$ to decide acceptance or rejection. We construct a two-turn quantum verifier W for the new quantum $(k+1)$-prover interactive proof system for L. The constructed prover W starts with generating a random string r of length q_{M} in the first turn, and sends r to the first k provers. W does not send any question to the last prover. In the second turn W receives N_i from the ith prover expecting the original second message from the original ith prover, for $1 \leq i \leq k$. From the $(k+1)$-st prover W receives k quantum registers $\mathsf{M}_1, \ldots, \mathsf{M}_k$, expecting the original first messages of the original k provers. W then proceeds like V would. The details and the analysis are relegated to the full version of this paper [16]. □

Now Theorem 1 follows from Theorem 4 and Lemmas 14 and 15. Corollary 6, claiming $\text{QIP} \subseteq \text{QMIP}(2, 2, 1, 2^{-p})$ for any $p \in \text{poly}$ follows directly from Lemma 15 and the fact shown by Marriott and Watrous [20] that any language in QIP can be verified by a three-message public-coin quantum interactive proof system of perfect completeness with exponentially small error in soundness (i.e., $\text{QIP} \subseteq \text{QMAM}(1, 2^{-p})$ for any $p \in \text{poly}$).

References

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proc. 13th ACM STOC*, pages 20–30, 1998.

[2] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[3] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[4] L. Babai. Trading group theory for randomness. In *Proc. 17th ACM STOC*, pages 421–429, 1985.

[5] L. Babai, L. J. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[6] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proc. 20th ACM STOC*, pages 113–131, 1988.

[7] J.-Y. Cai, A. Condon, and R. J. Lipton. PSPACE is provable by two provers in one round. *J. Comput. Syst. Sci.*, 48(1):183–193, 1994.

[8] R. E. Cleve, D. Gavinsky, and R. Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive private information retrieval systems. arXiv.org e-Print archive, arXiv:0707.1729 [quant-ph], July 2007.

[9] R. E. Cleve, P. Høyer, B. F. Toner, and J. H. Watrous. Consequences and limits of nonlocal strategies. In *Proc. 19th Annual IEEE Conference on Computational Complexity*, pages 236–249, 2004.

[10] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Interactive proofs and the hardness of approximating cliques. *J. ACM*, 43(2):268–292, 1996.

[11] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems (extended abstract). In *Proc. 24th ACM STOC*, pages 733–744, 1992.

[12] L. J. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoret. Comput. Sci.*, 134(2):545–557, 1994.

[13] S. Goldwasser, S. Micali, and C. W. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[14] T. Ito, H. Kobayashi, D. Preda, X. Sun, and A. C.-C. Yao. Generalized Tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems. In *Proc. 23rd Annual IEEE Conference on Computational Complexity*, 2008.

[15] J. Kempe, H. Kobayashi, K. Matsumoto, B. F. Toner, and T. Vidick. Entangled games are hard to approximate. arXiv.org e-Print archive, arXiv:0704.2903 [quant-ph], 2007.

[16] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. arXiv.org e-Print archive, arXiv:0711.3715 [quant-ph], Nov. 2007.

[17] A. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[18] A. Kitaev and J. H. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proc. 32nd ACM STOC*, pages 608–617, 2000.

[19] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. Syst. Sci.*, 66(3):429–450, 2003.

[20] C. Marriott and J. H. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[21] A. Nayak and P. W. Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003.

[22] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[23] P. W. Shor. Fault-tolerant quantum computation. In *Proc. 37th FOCS*, pages 56–65, 1996.

[24] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit-commitment protocols. *Physical Review A*, 65(1):012310, 2002.

[25] J. H. Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoret. Comput. Sci.*, 292(3):575–588, 2003.

[26] J. H. Watrous. Zero-knowledge against quantum attacks. In *Proc. 38th ACM STOC*, pages 296–305, 2006.

[27] S. Wehner. Entanglement in interactive proof systems with binary answers. In *Proc. 23rd STACS*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171, 2006.