Entangled games are hard to approximate

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

Ben Toner‡
CWI, Amsterdam
The Netherlands

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

Abstract

We establish the first hardness results for the problem of computing the value of one-round games played by a verifier and a team of provers who can share quantum entanglement. In particular, we show that it is NP-hard to approximate within an inverse polynomial the value of a one-round game with (i) quantum verifier and two entangled provers or (ii) classical verifier and three entangled provers. Previously it was not even known if computing the value exactly is NP-hard. We also describe a mathematical conjecture, which, if true, would imply hardness of approximation to within a constant.

We start our proof by describing two ways to modify classical multi-prover games to make them resistant to entangled provers. We then show that a strategy for the modified game that uses entanglement can be "rounded" to one that does not. The results then follow from classical inapproximability bounds. Our work implies that, unless $\mathrm{P} = \mathrm{NP}$, the values of entangled-prover games cannot be computed by semidefinite programs that are polynomial in the size of the verifier's system, a method that has been successful for more restricted quantum games.

*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.

‡Part of this work was completed at Caltech. Supported by the National Science Foundation under Grants PHY-0456720 and CCF-0524828, by EU project QAP, by NWO VICI project 639-023-302, and by the Dutch BSIK/BRICKS project.

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

1 Introduction

Multi-prover games have played a tremendous role in theoretical computer science over the last two decades. In this setting, several provers, who are not allowed to communicate with each other during the game, exchange messages with a verifier according to a prescribed protocol and try to convince him to accept. The *value* of a game is the maximum probability with which the provers can achieve this, averaged over all the verifier's questions and possibly over the shared randomness of the provers. The Cook-Levin Theorem implies that it is NP-complete to compute the value of such a game, where the input is an explicit description of the game, i.e., a set of possible questions, possible answers, a distribution on questions and acceptance predicates for the verifier. A lot of research effort went into determining how hard it is to *approximate* the value of such games, culminating in the celebrated PCP Theorem [ALM$^+$98, AS98], which shows that the value of a two-prover one-round game with a constant number of possible answers is NP-hard to approximate to within some constant. This result has had wide-ranging applications, most notably in the field of hardness of approximation, where it is the basis of many optimal results.

When considering multi-prover games in the quantum world, the laws of quantum mechanics allow for a fascinating new effect: namely, the provers can share an arbitrary *entangled* state, on which they may perform any local measurements they like to help them answer the verifier's questions. The fact that entanglement can cause non-classical correlations is a familiar idea in quantum physics, introduced in a seminal 1964 paper by Bell [Bel64]. Most importantly, there is no physical way to prevent provers from sharing entanglement or to limit how much they have. Compare this to the restriction that the provers cannot communicate during the game, which can be enforced physically by separating the provers in space so that there is no time for a message to travel from one to the other. It is thus a natural and important question to ask how shared entanglement between the provers influences the value of the game, as entanglement can allow for new strategies of the provers. Notice that entanglement can potentially either make it easier or harder to approximate the value of a game, and it is a wide open question which of these two effects actually takes place. For example, no algorithm—of any complexity at all—is known to approximate the value of an arbitrary entangled-prover game. One of the most important questions in this field, which we answer in this paper, has been to determine if it is hard or easy to compute the value of entangled-prover games.

Two recent results give evidence that entangled-prover games might actually be computationally much *easier* than their classical counterparts. First, Cleve et al. [CHTW04] showed that in the case of a particular class of two-prover one-round games, XOR-games, the value when provers are entangled can be computed (to exponential precision) in polynomial time. In contrast, Håstad [Hås01] showed that for these games *without* entanglement it is NP-hard to approximate the value to within some constant. To prove their result, Cleve et al. show that the maximization problem of the two provers can be written as a semidefinite program (SDP) of polynomial size. It is well known that there are polynomial time algorithms to find the optimum of such SDPs up to exponential precision, and hence there is a polynomial time algorithm to compute the value of this game. More precisely, Cleve et al. show that there is an SDP relaxation for the value of the game with the property that its solution can be translated back into a protocol of the provers. This is possible using an inner-product preserving embedding of vectors into two-outcome observables due to Tsirelson [Tsi87], which works in the particular case of XOR-games. It has been a major open question whether this result generalizes beyond XOR-games.

In a second recent result giving evidence that entangled-prover games are easy, Kempe, Regev and Toner [KRT07] show that even for the class of *unique* games (which contains the class of XOR-games), an SDP-relaxation of the game gives a good approximation to its value. Hence, for unique games there is a polynomial time algorithm to *approximate* the value of the game to within a constant.

An SDP-relaxation is not specific to XOR-games or unique games and can be written for all entangled

two-prover games.[1] If the SDP is tight (as in the case of XOR-games) or close to tight (as in the case of unique games) there is a polynomial time algorithm to compute or approximate the value of the game. It was speculated that perhaps SDPs can compute or at least approximate well the value of an entangled game for more general games. The semidefinite programming approach has been widely successful whenever quantum communication is involved: for example Kitaev and Watrous [KW00] have shown that SDPs can exactly compute the value of *single*-prover quantum games, Gutoski and Watrous proved that the value of quantum refereed games is as hard to compute as the value of classical refereed games again via semidefinite programming [GW07], and Kitaev showed that the cheating probability for quantum coin-flipping protocols [Kit] can be computed by SDPs. Moreover, Navascues et al. [NPA07] recently gave a hierarchy of SDP relaxations to approximate the value of an entangled two-prover game; yet no bounds on the quality of approximation have been proved and these SDPs are in general not of polynomial size.

The major open question is thus to determine if it is easy or hard to compute or even to approximate the value of general entangled-prover games. In particular, would it be possible that the value of such games could be computed or approximated by an SDP?

Our results. In this paper we resolve the open question above by showing for the first time that it is NP-hard to compute the value of entangled multi-prover games in the quantum world. We need to distinguish between two types of entangled games: on one hand one can still restrict the (possibly entangled) provers to classical communication; we call such games *classical entangled games*. On the other hand one can also allow the provers to communicate *quantum* messages with a *quantum verifier*; we call these games *quantum entangled games*. In both cases the hardness of computing the value of the game with entangled provers was previously not known,[2] and we show NP-hardness in two cases: for two-prover one-round *quantum entangled games* (in the first part of the paper) and for three-prover one-round *classical entangled games* (in the second part). Then we proceed to show that even *approximating* the value of these two types of games is NP-hard, thus giving the first hardness of approximation results.[3] Our main result can be stated as follows:

Theorem 1. *There exists a polynomial p such that it is* NP*-hard to decide, for an explicitly given*

1. *two prover one-round quantum entangled game G or*
2. *three prover one-round classical entangled game G,*

whether its value is 1 *or* $1 - 1/p(|G|)$.[4]

This theorem implies that no polynomial-time algorithm can compute the value of an entangled game to within polynomial precision. Given the importance of SDPs in results on entangled games, the following immediate corollary is of interest:

Corollary 2. *The success probability of classical entangled* 3*-prover or quantum entangled* 2*-prover games cannot be computed by SDPs of polynomial size, unless* $\mathrm{P} = \mathrm{NP}$.

The results above leave open the case of *two*-prover one-round *classical* entangled games. In the third part of this paper we give a hardness result for this type of game which is stated precisely in Section 5 in the setting of *succinct* games and interactive proofs; here we just give a brief overview. This third result has a

[1] In particular it will also be a relaxation for the value of the classical game (which is not tight in this case, unless $\mathrm{P} = \mathrm{NP}$).

[2] Kobayashi and Matsumoto [KM03] showed that when the communication and the verifier are quantum, but the provers do not share any entanglement, then the resulting games behave like classical games without entanglement, i.e., it is NP-hard to approximate their value to within a constant.

[3] Obviously the hardness of computation result is implied by the hardness of approximation result. We include it nonetheless in Sec. 3.1 for the quantum entangled games to illustrate the main ideas.

[4] See Section 2 for a precise definition of the size $|G|$ of G.

slightly different flavor: we scale up to games with exponential number of questions and answers, but given succinctly (i.e. the game is given by a description of the circuit of the verifier of size polynomial in $\log |Q|$, the length of the questions). For these games we show that to approximate the value to within an inverse polynomial (in $\log |Q|$) is at least as hard as to approximate to within a constant the value of classical *single*-prover *multi-round* games with polynomial rounds. Note that this is a better approximation than in the first two results of our paper (where the approximation was an inverse polynomial in $|Q|$), but our hardness in this case is weaker than in the previous two results. In particular, combining this with an adapted version of Shamir's result [Sha92] that IP $=$ PSPACE, our result implies PSPACE$\subseteq$ MIP$^*(2,1)_{1,1-\mathrm{poly}^{-1}}$. Again, no such result was previously known for these games.

All three results turn out to have something in common—in the analysis of all three of them we show that by enforcing certain tests we obtain sets of projectors (which characterize the strategy of the provers) which pairwise *"almost commute"*. From this condition we need to derive a classical strategy for the original classical game, and we do this in a similar fashion in all three cases.

Proof ideas and new techniques.

Reduction: We prove our NP-hardness results by a reduction from the hardness of approximation result for classical (non-entangled) games, as implied by the PCP Theorem, which we state in the language of games:

Theorem (PCP Theorem [ALM$^+$98, AS98])**.** *There is a constant $s < 1$ such that it is* NP*-hard to decide, given a two-prover one-round game with a constant number of answers, whether its value is* 1 *or* $\leq s$*.*

We start with an instance of such a classical two-prover one-round game and modify it to a two-prover one-round quantum entangled game (or a three-prover classical entangled game, in the second part of this paper) with the property that the value of the new entangled game is at least as big as the value of the original game. In other words, if the value of the original game is 1, the value of the new game is still 1. To show that it is NP-hard to *compute* the value of the entangled game we need to show that if the value of the original game is below s then the value of the new entangled game is *smaller* than 1. In particular, it suffices to show that if the value of the new entangled game is 1, then the value of the original game is also 1. To show this, we use a successful strategy of the entangled provers to construct a strategy in the original game that achieves a large value (see *Rounding* below).

Because we only need to show this when the new value is *exactly* 1 our task is fairly easy once we have established how to modify the game. It requires substantially more work to prove the hardness of approximation result. We perform the same reduction as in the exact case, but now we need to show that if the value of the original game is at most s, then the value of the new entangled game is bounded away from 1 by an inverse polynomial. Equivalently, we have to show that if the value of the new entangled game is above $1 - \varepsilon$ for some inverse polynomially small ε, then the value of the original classical game is *larger* than s.

Modify the game to "immunize" against entanglement: An essential novel technique in our paper is the design of the new games used in our reduction. We design the new games in a way that limits the cheating power of entangled provers. To this end—and this is a crucial difference to previous attempts to upper bound the value of entangled games—we add an extra test to the game. This new test, which can be added generically to *any* two-prover one-round game, significantly limits the use of entanglement by the provers beyond its quality as shared randomness. We hope that this technique of "immunizing" a game against entanglement can be extracted to serve a wider purpose in other contexts where we want to limit the power of entanglement, possibly with cryptographic applications.

In hindsight the fact that we need to modify the games comes as no surprise. Several classical games have been analyzed in the past to show that without modification of the game, entanglement drastically increases their value. One striking example is given by the Magic Square game [Ara02]: Two classical

players can win this game with probability at most $17/18$. However, when given entanglement, the players can win *perfectly*, i.e., they have a strategy that wins with probability 1.

Our next novel element is the actual design of the new test. The difficulty is to show that entanglement does not help the provers to coordinate their replies to increase the success probability. In the case of quantum games (in the first part of this paper) our idea is to astutely use *quantum* messages and *quantum* tests, and in particular a version of the SWAP-test, to enforce (approximately) that the provers do not entangle the message register with the entangled state they share. This allows us to get conditions that involve the provers' operators (describing their strategies) on two *different* questions. For this it is crucial that the messages are quantum; we do not see any way to achieve this result for classical messages.

When we analyze classical entangled games (in the second part of our paper) we design a different test: we modify the game by introducing a *third* player. We use the extra player to introduce a consistency test that forces two of the provers to give the *same* answer. As a result, to pass this test, the two original players can only use an entangled state of a specific form; it must be (approximately) *extendable*, i.e., it must be the density matrix of a symmetric tripartite state. There are prior results pointing to the potential usefulness of a third player to limit the cheating power of entanglement. For example, two entangled provers can cheat in the Odd Cycle game of Ref. [CHTW04], but if we add a third prover, then entangled provers can perform no better than classical ones [Ton06]. Moreover, after the completion of this work we have learned from A. Yao [Yao] about a way to add a third player to the Magic Square game such that as a result the winning probability of entangled provers is ≈ 0.94.

For our third result on two-prover classical entangled games, our reduction has the same spirit and similar analysis as in the previous two cases: here we start with a *single*-prover multi-round game and modify it to a one-round game by introducing a second prover to prevent the first prover to entangle the answers of subsequent rounds. Our modification here mimics a construction of [CCL94] used to prove that PSPACE has (non-entangled) two-prover one-round systems.[5]

Rounding: The extra quantum test (resp., the extra player) allows us to extract a mathematical condition on the operations of the entangled players. More precisely it turns out that the projectors corresponding to the various questions of the verifier pairwise "almost commute" in some sense or "almost do not disturb" the entangled state. This means that the provers' actions are "almost classical", in the sense that they allow us to take any strategy in the entangled game and convert it back to a strategy in the original classical game. We call this conversion *rounding* from a quantum solution to a classical solution, in analogy to the rounding schemes used to convert a solution to an SDP relaxation to a solution of the game. To explain the idea of our new rounding scheme, assume that the provers, when receiving a question from the verifier, perform a projective measurement on their share of the entangled state depending on the question, and answer with the outcome they get (it will turn out that this is essentially what the provers can do, even when the game involves quantum communication). In the *exact* case, when the value of the entangled quantum game is 1, the measurements corresponding to different questions *commute* exactly. Hence, there is a common basis in which the projectors corresponding to different answers are all diagonal for all questions. In other words, for each question, the projectors simply define a partition of the basis vectors. The probability that the provers give a certain pair of answers just corresponds to the size of the overlap of the supports of the two corresponding projectors, i.e., to the number of basis vectors that are contained in both of them. We can now construct a classical strategy for the original game, where the provers use shared randomness to sample a basis vector, check which projector/partition contains it, and output the corresponding answer. This classical strategy achieves exactly the same probability distribution on the answers, and hence the same value of the game.

Matters complicate in the case where the value of the entangled game is $1 - \varepsilon$. Now, the provers' mea-

[5] In fact, we show that the [CCL94] construction still remains sound even with entangled provers, albeit with a weaker soundness than in the classical case.

surements corresponding to different questions "almost commute". To exploit this property in a rounding scheme, imagine the following pre-processing step to eliminate entanglement from the strategy: Before the game starts, the provers apply in sequence all possible measurements, corresponding to all possible questions, on a share of the entangled state, and write down a list of all the answers they obtain.[6] Then, during the game, when they receive a question from the verifier, they respond with the corresponding answer in their list. Because the measurements almost commute, the answer to any one particular question in this sequential measurement scheme are similarly distributed to the scenario in the entangled game, where the prover only performs the one measurement corresponding to that question. This can be seen by "commuting" the corresponding projectors through the list of projectors in the measurement, where each time we commute two operators we loose an ε in precision. As a result, also the success probability of this new unentangled strategy is similar to the one in the entangled game, or at least not too low.

A new mathematical challenge: As mentioned above, our tests enforce an almost-commuting condition on the operators of the provers. If they would commute exactly, they would be diagonal in a common basis, which means that the strategy is essentially classical and does not use entanglement. If one could conclude that the operators are *nearly diagonal* in some basis, one could again extract a classical strategy as in the exact case. Hence we reduce proving *constant* hardness of approximation to the question whether one can approximate our operators by commuting ones. This touches upon a deep question in operator algebra: *Do almost commuting matrices nearly commute?* Here *almost commuting* means that the commutator is small in some norm, and nearly commuting means that the matrices can be approximated by matrices that are diagonal in some common basis. This famous question was asked for *two Hermitian* matrices by Halmos back in 1976 [Hal76].[7] It was shown subsequently [Voi83],[8] using methods from algebraic topology, that this conjecture is false for two *unitary* matrices. Then, Halmos' conjecture was disproved in the case of three Hermitian matrices. Finally Halmos' conjecture was proved [Lin97] by a "long tortuous argument" [DS01] using von Neumann algebras, almost 20 years after the conjecture had been publicized. In our case we reduce proving hardness of approximation of the value of an entangled game to the conjecture for a set of pairwise almost commuting *projectors*, where the norm is the Frobenius norm $\|A\|_2^2 = \mathrm{Tr}(A^\dagger A)$ (see Sec. 3.1):

Conjecture. *Let $W_1, \ldots, W_n$ be d-dimensional projectors such that for some $\varepsilon \geq 0$ for all $i, j \in \{1, \ldots, n\}$ $\frac{1}{d}\|W_i W_j - W_j W_i\|_2^2 \leq \varepsilon$. Then there exists a $\delta \geq 0$, and pairwise commuting projectors $\tilde{W}_1, \ldots \tilde{W}_n$ such that $\frac{1}{d}\|W_i - \tilde{W}_i\|_2^2 \leq \delta$ for all $i \in \{1, \ldots, n\}$.*

Our proof shows that the conjecture with a constant δ implies hardness of approximation of the value of entangled games to within a *constant*, i.e., best possible. For two, three or a constant number of projectors the conjecture is easy to prove for a constant δ. We do not know if it is true in general.

Related work. A subset of the authors has obtained weaker results on harness of approximation of the value of entangled two-prover *quantum* games, posted to the arXiv earlier [KV06]; the present paper includes and supersedes these results. Since this paper had been made public, our techniques have already been applied by [IKP$^+$07] to show similar results for *binary* three-player one-round classical entangled games. [IKP$^+$07] also give a new upper-bound for the value of these games; or, as often called in this context, they gave a new tripartite Tsirelson-inequality. After the completion of this work Cleve, Gavinsky and Jain [CGJ07] use a connection to private information retrieval schemes to show that succinctly given binary entangled classical games can not be approximated in polynomial time. Their result does not apply

[6] Obviously, the provers do not really need any entanglement to do this: all they have to do is sample from the joint distribution that corresponds to the distribution of all the answers in this sequence of measurements.

[7] For the operator norm.

[8] For a simpler, elegant proof see [EL89].

for explicitly given games, as it is based on an exponential expansion of the message length. It uses very different techniques, and is not comparable to ours.

Structure: The structure of this paper is as follows: In Section 2 we introduce the necessary definitions and notations we use. In Section 3 we prove our results on the NP-hardness of quantum entangled two-prover games. To flash out the ideas, we first prove hardness of *computing* the value of such games, before showing hardness of approximation. In Section 4 we show NP-hardness of approximation for the value of three-prover classical entangled games, and in Section 5 we give our hardness results for two-prover classical entangled games. We discuss our results and open questions in Section 6.

2 Preliminaries

We assume basic knowledge of quantum computation [NC00].

Games. In this paper we study multi-prover games, or cooperative games with imperfect information (henceforth *games*). We will only deal with one-round games played by N cooperative provers against a verifier. For an integer K, denote $\{1, \ldots, K\}$ by $[K]$.

Definition 3. *Let Q and A be integers. A game $G = G(N, \pi, V)$ is given by a set $\bar{Q} = \{q_{i_1 \ldots i_N}\}_{(i_1 \ldots i_N) \in [Q]}$ of questions and $\bar{A} = \{a_{i_1 \ldots i_N}\}_{(i_1 \ldots i_N) \in [A]}$ of* answers*, together with a distribution $\pi : [Q]^N \to [0, 1]$, and a function $V : [A]^N \times [Q]^N \to \{0, 1\}$.[9] The value of the game is*[10]

$$\omega(G) = \sup_{W_1, \ldots, W_N} \sum_{i_1, \ldots, i_N \in [Q]^N} \pi(i_1, \ldots, i_N) \sum_{j_1, \ldots, j_N \in [\bar{A}]^N} \Pr(a_{j_1 \cdots j_N}) V(a_{j_1 \cdots j_N} | i_1 \cdots i_N), \qquad (1)$$

where the W_i are the prover's strategies, and the probability $\Pr(a_{j_1 \cdots j_N}) = \Pr(W_1(i_1, r) \cdots W_N(i_N, r) = a_{j_1 \cdots j_N})$ is taken over the randomness of the provers.

The game G is played as follows: The verifier samples $i_1, \ldots, i_N$ from $[Q]^N$ according to π, and prepares a question $q_{i_1 \cdots i_N} \in \bar{Q}$. He sends the k-th part of the question to prover k for $1 \leq k \leq N$ and receives the answer $a_{j_1 \cdots j_N} \in \bar{A}$ from the provers. The provers win the game if $V(a_{j_1 \cdots j_N} | i_1 \cdots i_N) = 1$; otherwise the verifier wins. The *value* of a game is the maximum winning probability of the provers. The provers can agree on a strategy before the game starts, but are not permitted to communicate after receiving questions.

We distinguish three different kinds of games, based on the classical or quantum nature of the verifier, the provers, and the question and answer sets. A game G will be called

- *classical* if the verifier, the prover, and the question and answer sets are classical. In this case $q_{i_1 \cdots i_N} = (q_1, \ldots, q_N)$ and $a_{i_1 \cdots i_N} = (a_1, \ldots, a_N)$ are N-tuples, i.e., the verifier simply sends q_k to the k-th prover and receives a_k from him. We identify $\bar{Q}$ with $[Q]^N$, $\bar{A}$ with $[A]^N$, i_k with q_k, and j_k with a_k and often write Q for $[Q]$ and A for $[A]$. The strategies W_i are simply functions $W_i : Q \times R \to A$ where R is some arbitrary domain ("shared randomness"). In fact we can assume the strategies to be *deterministic*: there is always some $r \in R$ that maximizes the winning probability and we can fix it in advance.

- *classical entangled* if the verifier, and the question and answer sets are classical, but the provers are quantum, and are allowed to share an a priori entangled state $|\Psi\rangle$ of arbitrary dimension. This

[9] We write $V(\cdot, \cdot)$ as $V(\cdot|\cdot)$ to clarify the role of the inputs.

[10] We use a supremum because the optimal strategies might not be finite in the case of entangled provers.

increases the set of possible strategies to quantum operations performed on the prover's share of the entangled state. By standard purification techniques (see, e.g, [CHTW04]) one can assume that each prover performs a projective measurement $\mathcal{W}_q = \{W_q^a\}_{a\in A}$ with outcomes in A (i.e., $\sum_{a\in A} W_q^a = \mathrm{Id}$ and $(W_q^a)^\dagger = W_q^a = (W_q^a)^2$), where we adopt the same notational identifications as for classical games. We will use a superscript $*$ to indicate entangled-prover games. The value $\omega^*(G)$ of such a game is given by Eq. (1) where the probability $\Pr(a_1\, ldots, a_N) = \langle\Psi|(W_1)_{q_1}^{a_1} \otimes \cdots \otimes (W_N)_{q_N}^{a_N}|\Psi\rangle$.

- *quantum entangled* if both the verifier and the provers are quantum, and they exchange quantum messages. We usually denote such a game by G_q. In that case $q_{i_1\cdots i_N} \in \bar{Q}$ is a joint density matrix and the verifier sends its k-th part to the k-th prover for $1 \le k \le N$ using a quantum channel, possibly keeping a part in his own private register. After receiving as answer an N-register quantum state $a_{j_1\cdots j_N} \in \bar{A}$, where the k-th prover sends the k-th register, the verifier performs a quantum operation V' (which might depend on the questions in $[Q]^N$) on the answer and his private space, followed by a measurement $\{\Pi_{acc}, \Pi_{rej}\}$ of his first qubit. By purification we can assume that the kth prover performs a unitary transformation U_k on the message register and his part of the entangled state $|\Psi\rangle$ and then sends the message register back to the verifier. The value of an entangled-prover quantum game, ω_q^*, is given by Eq. (1) where

$$\sum_{j_1,\ldots,j_N} \Pr(a_{j_1\cdots j_N}) V(a_{j_1\cdots j_N}|i_1\ldots i_N) = \mathrm{Tr}(\Pi_{acc} V'(U_1 \otimes \cdots \otimes U_N)(q_{i_1\cdots i_N} \otimes |\Psi\rangle\langle\Psi|)).$$

Input size. A game is described by Q, A, π and V, and hence our complexity parameter, the size of the input, is polynomial in Q and A.[11] We will always assume that the description of the distribution π is of polynomial size in Q. In the case of quantum games we also have to take into account the size of a description of the question $q_{i_1\ldots i_N}$, and the verification procedure V', and the dimension of the answer $a_{j_1\ldots j_N}$: we always assume that the dimensions of $q_{i_1\ldots i_N}$ and $a_{j_1\ldots j_N}$ are polynomial in Q and A and hence there is a (classical) description of $q_{i_1\ldots i_N}$ and of V' (which can be assumed to be a unitary of polynomial dimension) of polynomial size in Q, A.[12]

Symmetric games. For convenience we will work with symmetric distributions π. The next lemma shows why this poses no restriction (we only need the case of 2 provers).

Lemma 4. *For every game $G = G(2, \pi, V)$ there is a game $G' = G(2, \pi', V')$ of the same value and twice as many questions, such that π' and V' are symmetric under permutation of variables. Moreover there is an optimal symmetric strategy for G'.*

Proof. The verifier V' in game G' samples q, q' from π. He adds an extra bit register to the questions and with probability $1/2$ he sends $(q, 1)$ to prover 1 and $(q', 2)$ to prover 2, otherwise he swaps the two questions. In the second case he swaps the received answers and in both cases applies the predicate V. For the lower bound observe that if S_1, S_2 is a strategy for G, then the strategy for G' where each prover applies S_i if his second message bit is i fares as well as S_1, S_2 (and is symmetric). For the upper bound note that from any strategy S_A, S_B for G' we can construct a strategy for G that fares at least as well, by choosing the better of either $S_A(\cdot, 1), S_B(\cdot, 2)$ or $S_B(\cdot, 1), S_A(\cdot, 2)$. Moreover, V' is obviously symmetric under permutation of question-answer pairs. □

In the case where the provers are allowed to share entanglement, we can assume that if π and V have some symmetry, it is mirrored in the optimal prover's strategies:

[11] Here we always assume that N is a constant.

[12] In fact all games we consider also have a circuit of size $\mathrm{poly}\log Q$ to prepare $q_{i_1\ldots i_N}$ from $i_1, \ldots, i_N$.

Lemma 5. *Let $G = G(N, \pi, V)$ be a (classical or quantum) entangled-prover game, such that $\pi(i_1, \ldots, i_N)$ is symmetric in $i_1, \ldots, i_k$ and V is symmetric under simultaneous permutation of the registers $1 \ldots k$ of the questions $q_{i_1 \cdots i_N}$ and of the answers $a_{i_1 \cdots i_N}$ for $k \leq N$. Then given any strategy $P_1, \ldots, P_N$ with entangled state $|\Psi\rangle$ that wins with probability p, there exists a strategy $P'_1, \ldots, P'_N$ with entangled state $|\Psi'\rangle$ and winning probability p such that $P'_1 = \ldots = P'_k$ and $|\Psi'\rangle$ is symmetric with respect to the provers $1, \ldots, k$.*

Proof. Let $\mathfrak{S}_k$ be the set of permutations of $\{1, \ldots, k\}$ and assume, by appropriately padding with extra qubits, that the first k registers of $|\Psi\rangle$ have the same dimension. Define strategies $P'_1, \ldots, P'_N$ as follows: the provers share the entangled state $|\Psi'\rangle = \sum_{\sigma \in \mathfrak{S}_k} |\sigma(1)\rangle \ldots |\sigma(k)\rangle \otimes |\Psi^\sigma\rangle$, where the register containing $|\sigma(i)\rangle$ is given to prover i and $|\Psi^\sigma\rangle$ is obtained from $|\Psi\rangle$ by swapping the first k registers according to σ. For $i \leq k$ prover i measures the register containing $|\sigma(i)\rangle$ and applies $P_{\sigma(i)}$. For $i > k$, $P'_i = P_i$. By symmetry of π and V this new strategy achieves the same winning probability p, and $|\Psi'\rangle$ has the required symmetry properties. □

3 Hardness of two-prover entangled quantum games

In this section we prove Theorem 1 for the case of two-prover quantum entangled games. To better quantify the dependence on the input size, we restate it as a separate result:

Theorem 6. *There is a constant $s_q > 0$ such that it is* NP*-hard to decide, given an two-prover quantum entangled game, whether its value is* 1 *or less than* $1 - \varepsilon$ *for* $\varepsilon = \frac{s_q}{|Q|^4}$.

As mentioned in the introduction, we will prove this by a reduction from the PCP Theorem. However, to more clearly and cleanly expose the ideas in this proof, we will first prove the simpler statement about NP-hardness of *computing* the value.

3.1 NP-hardness of computing the value of entangled quantum games

Theorem 7. *It is* NP*-hard to decide, given an two-prover quantum entangled game, whether its value is* 1.

We first describe how to modify a two-prover classical game $G_c(2, \pi, V)$ with questions Q and answers A to a two-prover *quantum* game of equal or higher value. We assume that the distribution $\pi(q, q')$ is symmetric (as per Lemma 4, at the expense of doubling the number of questions) and also that there is a non-zero probability for each question to be asked (otherwise we remove it from Q without affecting the value of the game).

The modified quantum game. In the constructed quantum game G_q the verifier sends quantum registers $|q, 0\rangle_A$ and $|q', 0\rangle_B$ to provers A and B. We call the first part of this register the *question register* and the second part the *answer register*. The answer register is initially in some designated state $|0\rangle$ and the provers are expected to write the answers $a \in A$ to the question $q \in Q$ into this register and then send both registers back. The verifier performs one of two tests, with equal probability:

Classical Test: The verifier samples (q, q') according to the distribution $\pi(q, q')$, and sends $|q, 0\rangle$ to prover A and $|q', 0\rangle$ to prover B. Upon receiving these registers from the provers, he measures them and accepts if the results of the measurement of the question registers is q, q' and the results of the measurement of the answer registers a, a' would win the game G_c.

Quantum Test: The verifier samples (q, q') according to the distribution $\pi(q)\pi(q')$, where $\pi(q)$ is the marginal of $\pi(q, q')$ and prepares the state

$$\frac{1}{\sqrt{2}} \left(|0\rangle |q, 0\rangle_A |q', 0\rangle_B + |1\rangle |q', 0\rangle_A |q, 0\rangle_B \right). \tag{2}$$

He keeps the first qubit and sends question and answer registers to provers A and B. Upon receiving these registers from the provers, he performs a controlled-SWAP on registers A and B conditioned on the first qubit being $|1\rangle$ (he swaps both the question and the answer register). Then he measures his qubit in the basis $\{|+\rangle, |-\rangle\}$[13] and the question registers. He accepts iff the results of the measurement of the question registers is q, q' and the outcome of the measurement of the first qubit is "+".

Remarks: Note that the value $\omega_q^*(G_q)$ of the constructed game G_q is obviously at least the value of G_c: If the entangled quantum provers, controlled on the question, simply write the answer that the classical unentangled provers would have given into the answer register, they always pass the quantum test, and hence $\omega_q^*(G_q) \geq \omega(G_c)/2 + 1/2 \geq \omega(G_c)$.

Moreover the description of the quantum game has essentially the same size as the description of the classical game, i.e. the complexity parameter is the same in both cases. The dimension of question and answer registers is $|Q|$ and $|A|$ and the SWAP test only requires extra space that is no more than linear in the number of qubits swapped.

Note that it is only the SWAP-test that is genuinely quantum, and allows us to show that the provers cannot entangle too much the questions they receive with the entangled state they share, by relating their actions on two different messages. This test has been used in various settings in the past. In its most simple form it was used in [BCWdW01] to give a protocol for quantum fingerprinting. However, the test that we perform here is a little more sophisticated, since it implements only a *partial* SWAP on the two message registers, which might be entangled with the prover's private spaces and entanglement, on which the verifier in unable to perform the swapping. This partial swap has been used in [KW00] to show parallelization for QIP, and in [KMY03] to prove the inclusion QMA(3) $\subset$QMA(2), where the 2 and 3 refer to the number of Merlins.

A last remark concerns the two different probability distributions used in the two tests. We really need to change the distribution in the quantum test, because it gives us a commutation condition for *all* operators of the provers, corresponding to all different questions. Otherwise, we would only obtain it for pairs of questions q, q' corresponding to a non-zero $\pi(q, q')$, which is not sufficient to round to a classical strategy.

Existence of a good classical strategy. We now show that if the value of the quantum game is 1, then there is a strategy for the classical game that wins with probability 1.

Lemma 8. *If $\omega_q^*(G_q) = 1$ then $\omega(G_c) = 1$.*

This implies that if the value of the classical game was less than 1, then the value of the quantum game is less than 1. Since it is NP-hard to distinguish whether the value of the classical game is 1 or not, it follows that it is NP-hard to decide whether the value of the quantum game is 1.

Proof of Lemma 8: Consider a maximizing strategy, which in particular passes the quantum test with certainty.[14] Note that if it were not for the controlled-SWAP the game would be essentially an entangled *classical* game, because question and answer registers are prepared in a classical state and are immediately measured when received by the verifier. We first show that the strategy of the provers is indeed essentially a classical entangled strategy.

Claim 9. *There is a shared bipartite state $|\Psi\rangle_{AB}$ and for each question $q \in Q$ a set of projectors $\{W_q^a\}_{a \in A}$ acting on each prover's half of $|\Psi\rangle$ with $\sum_{a \in A} W_q^a = \mathrm{Id}$ such that each provers' transformation can be*

[13] Or, equivalently, he performs a Hadamard transform and measures his qubit in the standard basis.

[14] Strictly speaking it could be that such a strategy exists only in the limit of infinite entanglement, so we would have to use a strategy that achieves success probability arbitrarily close to 1. Since in this part we only give the ideas of the rigorous proof in Section 3.2, we ignore this issue.

written as $|q\rangle|0\rangle|\Psi\rangle \to |q\rangle \sum_a |a\rangle W_q^a|\Psi\rangle$ *and the probability that the verifier measures* a, a' *in the answer registers given he sampled* q, q' *in the classical test is*

$$p_q(a, a'|q, q') = \|W_q^a \otimes W_{q'}^{a'}|\Psi\rangle_{AB}\|^2.$$

Proof. At the beginning of the protocol the provers share some entangled state $|\Psi'\rangle$ (including their private workspace). From Lemma 5 we can assume that the strategies in the quantum game are symmetric, i.e., that A and B apply the same unitary transformation U. Since the provers pass the quantum test perfectly it means that they do not change the question register. Hence it is easy to see that U is block-diagonal and can be written as $U = \sum_q |q\rangle\langle q| \otimes U_q$ where U_q acts on the answer register and half of $|\Psi'\rangle$. Define the operators $\tilde{W}_q^a = \langle a|U_q|0\rangle$, where $|0\rangle$ and $|a\rangle$ only act on the answer register, not on $|\Psi'\rangle$, i.e. $U_q|0\rangle|\Psi'\rangle = \sum_a |a\rangle\tilde{W}_q^a|\Psi'\rangle$. Then it follows that $\sum_a (\tilde{W}_q^a)^\dagger \tilde{W}_q^a = \mathrm{Id}$, meaning that $\tilde{W}_q^a$ are superoperators acting on a part of $|\Psi'\rangle$. By standard arguments we can now enlarge the system to a state $|\Psi\rangle$ such that we can replace the $\tilde{W}_q^a$ by projectors W_q^a which give exactly the same outcome probabilities. □

We now derive the crucial condition that allows us to define a good classical strategy.

Claim 10.

$$\forall q, q', a, a' \quad W_q^a \otimes W_{q'}^{a'}|\Psi\rangle = W_{q'}^{a'} \otimes W_q^a|\Psi\rangle.$$

Proof. After the controlled-SWAP and the measurement of the question registers as q, q', the remaining state of the entire system can be described as

$$\begin{aligned}
&\frac{1}{\sqrt{2}} \sum_{a,a'} |a\rangle|a'\rangle \left(|0\rangle(W_q^a \otimes W_{q'}^{a'})|\Psi\rangle + |1\rangle(W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle\right) \\
&= \frac{1}{2} \sum_{a,a'} |a\rangle|a'\rangle \left(|+\rangle(W_q^a \otimes W_{q'}^{a'} + W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle + |-\rangle(W_q^a \otimes W_{q'}^{a'} - W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle\right)
\end{aligned}$$

and hence the probability to measure "$-$" in the extra qubit is $\frac{1}{4}\sum_{a,a'} \|(W_q^a \otimes W_{q'}^{a'} - W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle\|^2$ which must be 0 since the provers pass the quantum test with certainty. □

Rounding: This property of the projectors can be expressed in a different fashion. Assume for simplicity that the shared state is maximally entangled, i.e., $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_A|i\rangle_B$, and that all projectors are real. Then for any such projectors W, W' we have $\|W \otimes W'|\Psi\rangle\|^2 = \frac{1}{d}\|WW'\|_F^2$, where $\|A\|_F^2 = \mathrm{Tr}(A^\dagger A)$ is the Frobenius norm. The condition in Claim 10 can be rewritten as $\frac{1}{d}\|W_q^a W_{q'}^{a'} - W_{q'}^{a'} W_q^a\|_F = 0$, i.e. the two projectors *commute*. Hence, in some basis $\{|e_i\rangle\}_{i=1}^d$, all W_q^a are diagonal matrices with only 1 and 0 on the diagonal. In other words, each projector simply defines a *partition* of the basis vectors, and $p(aa'|qq') = \frac{1}{d}\|W_q^a W_{q'}^{a'}\|_F^2$ just measures the relative *overlap* of the two partitions. With this in mind we can easily design a classical randomized strategy for G_c with the same success probability. The provers sample a shared random number $i \in \{1, \ldots, d\}$. When receiving question q they answer with a such that the basis vector $|e_i\rangle$ is in the support of W_q^a.

This proof can be generalized to an arbitrary shared state $|\Psi\rangle$ and general projectors. We will not give the full details (in any case Thm. 7 follows from Thm. 6), but the way to prove this is to define a diagonal real positive matrix D with the Schmidt-coefficients of $|\Psi\rangle$ in the diagonal. Then $\|W \otimes W'|\Psi\rangle\|^2 = \|WDW'^T\|_F^2$, where the elements on the diagonal of D can be thought of as weights, and the condition in Claim 10 becomes $\|W_q^a D(W_{q'}^{a'})^T - W_{q'}^{a'} D(W_q^a)^T\|_F = 0$. Moreover, following the same ideas as used in Claim 14 to show Eq. (3b), we obtain $\|W_q^a D - D(W_q^a)^T\|_F = 0$. Together these conditions imply $W_q^a W_{q'}^{a'} D = W_{q'}^{a'} W_q^a D$, i.e. the two projectors commute over the space where D is non-zero. The classical strategy is now a weighted version of the strategy outlined in the case of a maximally entangled shared state. □

3.2 NP-hardness of approximating the value of entangled quantum games

With the intuitions obtained so far we can now tackle the harder case of hardness of approximation. First a quick overview. We modify the game in exactly the same way as before. To prove Theorem 6 we now need to show, for s from the PCP Theorem:

Lemma 11. *If $\omega_q^*(G_q) > 1 - \varepsilon$ then $\omega(G_c) > s$.*

This implies that if the value of the classical game was less than s, then the value of the quantum game is less than $1 - \varepsilon$. Since, from the PCP Theorem it is NP-hard to distinguish whether the value of the classical game is 1 or less than s, it follows that it is NP-hard to decide whether the value of the entangled quantum game is 1 or below $1 - \varepsilon$.

To prove Lemma 11, we first show that the strategies of the provers are essentially projective measurements (Claim 12). We then extract the "almost commuting" conditions on the operators of the provers (Claim 14), which allow us to give a good strategy for the original game.

Proof of Lemma 11. Consider a maximizing strategy.[15] It must pass each of the two tests with probability at least $1 - 2\varepsilon$. Again it is (approximately) true that the strategy of the provers is essentially an entangled *classical* strategy.

Claim 12. *There is a shared bipartite state $|\Psi\rangle_{AB}$ and for each question $q \in Q$ a set of projectors $\{W_q^a\}_{a \in A}$ acting on each prover's half of $|\Psi\rangle$ with $\sum_{a \in A} W_q^a = \mathrm{Id}$ such that if we replace each prover's transformation by $|q\rangle|0\rangle|\Psi\rangle \to |q\rangle \sum_a |a\rangle W_q^a |\Psi\rangle$ then the probability to pass each of the tests is at least $1 - 6\varepsilon$ and the probability distribution on the answers in the classical test is given by*

$$p_q(aa'|qq') = \|W_q^a \otimes W_{q'}^{a'} |\Psi\rangle\|^2.$$

Proof. As in the proof of Claim 9 the provers apply the same unitary transformation U, which now is not exactly block-diagonal, but in general can be written as $U = \sum_{q,\tilde{q} \in Q} |\tilde{q}\rangle\langle q| \otimes U_{q\tilde{q}}$. Because the verifier in both the classical and the quantum test measures q, q' in the answer register with probability at least $1 - 2\varepsilon$, this implies that

$$\mathrm{E}_{(q,q')} \left[\sum_{\tilde{q} \neq q} \sum_{\tilde{q}' \neq q'} \|U_{q\tilde{q}} \otimes U_{\tilde{q}'q'} |0\rangle_A |0\rangle_B |\Psi'\rangle_{AB}\|^2 \right] \leq 2\varepsilon,$$

for both when (q, q') is sampled according to $\pi(q, q')$ (from the classical test) or according to $\pi(q)\pi(q')$ (from the quantum test), where we have used symmetry of $|\Psi'\rangle$ for $\|\frac{1}{\sqrt{2}}(|0\rangle U_{q\tilde{q}} \otimes U_{\tilde{q}'q'} + |1\rangle U_{\tilde{q}'q'} \otimes U_{q\tilde{q}})|0\rangle_A |0\rangle_B |\Psi'\rangle_{AB}\|^2 = \|U_{q\tilde{q}} \otimes U_{\tilde{q}'q'} |0\rangle_A |0\rangle_B |\Psi'\rangle_{AB}\|^2$.

We approximate U by a block-diagonal unitary operator O_U as follows: extend each prover's private space by registers A' and B' of dimension $|Q|+1$, initialized to $|0\rangle_{A'}$ and $|0\rangle_{B'}$ and let $O_U = \sum_q |q\rangle\langle q| \otimes T_q$, where the unitary matrix T_q acts on half of the entangled state and the answer register (together shortened as $|\cdot\rangle$) and A' as

$$T_q|\cdot\rangle|0\rangle_{A'} = U_{qq}|\cdot\rangle|0\rangle_{A'} + \sum_{\tilde{q} \neq q} U_{q\tilde{q}}|\cdot\rangle|\tilde{q}\rangle_{A'}$$

and is extended to a unitary matrix on the other states $|q\rangle_{A'}$. Observe that

[15] Since it could be that the value of the game is only achieved in the limit of infinite entanglement we in fact consider a strategy with finite entanglement that has success probability $1 - \varepsilon - \delta$ for some arbitrarily small δ. We will not write this δ in what follows, but the proof goes through for small enough δ, for instance $\delta = O(\varepsilon)$.

$$\mathrm{E}_{(q,q')}\left[\|\big(O_U\otimes O_U-(U\otimes \mathrm{Id}_{A'})\otimes(U\otimes \mathrm{Id}_{B'})\big)|q,0\rangle_A|q',0\rangle_B|\Psi'\rangle|0\rangle_{A'}|0\rangle_{B'}\|^2\right]$$
$$=\mathrm{E}_{(q,q')}\left[2\sum_{(\tilde{q},\tilde{q}')\neq(q,q')}\|U_{q\tilde{q}}\otimes U_{q'\tilde{q}'}|0\rangle_A|0\rangle_B|\Psi'\rangle\|^2\right]\leq 4\varepsilon,$$

again for both when (q,q') is sampled according to $\pi(q,q')$ or according to $\pi(q)\pi(q')$. This means that for purposes of analysis we can replace Alice and Bob's transformation U by O_U, thereby replacing the transformation $U\otimes U$ on the message registers and $|\Psi\rangle$ by the transformation $O_U\otimes O_U$ on the message space and $|\tilde{\Psi}\rangle=|\Psi'\rangle|0\rangle_{A'}|0\rangle_{B'}$, at the expense of an error 4ε in statistical distance on the answer probabilities of the classical test and the outcome probabilities in the quantum test. Since O_U is block-diagonal, the remainder of this claim follows exactly as in the proof of Claim 9. □

The SWAP-test now allows us to establish a set of inequalities which capture the "almost commuting" property of the operators. In what follows we will repeatedly use the following easy to verify fact.

Fact 13. *Let $W^1,\ldots,W^k$ be projectors such that $\sum_i W^i=\mathrm{Id}$. Then $\sum_i\|W^i|\Psi\rangle\|^2=\||\Psi\rangle\|^2$ for any vector $|\Psi\rangle$.*

Claim 14.

$$\sum_{i,j=1}^{|Q|}\pi(q_i)\pi(q_j)\sum_{a_i,a'_j}\|(W^{a_i}_{q_i}\otimes W^{a'_j}_{q_j}-W^{a'_j}_{q_j}\otimes W^{a_i}_{q_i})|\Psi\rangle\|^2\leq 24\varepsilon, \tag{3a}$$

$$\sum_{i=1}^{|Q|}\pi(q_i)\sum_{a_i}\|(W^{a_i}_{q_i}\otimes\mathrm{Id}-\mathrm{Id}\otimes W^{a_i}_{q_i})|\Psi\rangle\|^2\leq 9\cdot 24\cdot\varepsilon. \tag{3b}$$

Proof. As in the proof of Claim 10, the left-hand side of (3a) is four times the probability to measure the first qubit in "$-$" in the quantum test. For (3b), using Fact 13, for any fixed q_j the following holds

$$\begin{aligned}\|(W^{a_i}_{q_i}\otimes\mathrm{Id}-\mathrm{Id}\otimes W^{a_i}_{q_i})|\Psi\rangle\|^2&=\sum_{a'_j,a''_j}\|(W^{a'_j}_{q_j}W^{a_i}_{q_i}\otimes W^{a''_j}_{q_j}-W^{a'_j}_{q_j}\otimes W^{a''_j}_{q_j}W^{a_i}_{q_i})|\Psi\rangle\|^2\\&\leq\sum_{a'_j,a''_j}\Big(\|(W^{a'_j}_{q_j}W^{a_i}_{q_i}\otimes W^{a''_j}_{q_j}-W^{a'_j}_{q_j}W^{a''_j}_{q_j}\otimes W^{a_i}_{q_i})|\Psi\rangle\|\\&\quad+\|(W^{a'_j}_{q_j}W^{a''_j}_{q_j}\otimes W^{a_i}_{q_i}-W^{a_i}_{q_i}\otimes W^{a''_j}_{q_j}W^{a'_j}_{q_j})|\Psi\rangle\|\\&\quad+\|(W^{a_i}_{q_i}\otimes W^{a''_j}_{q_j}W^{a'_j}_{q_j}-W^{a'_j}_{q_j}\otimes W^{a''_j}_{q_j}W^{a_i}_{q_i})|\Psi\rangle\|\Big)^2.\end{aligned}$$

We can bound the square of the sum of the three norms by 3 times the sum of the norms squared, and summing over a_i, averaging over q_i,q_j, and using $W^a_qW^{a'}_q=\delta_{a,a'}W^a_q$ for the second norm and Fact 13 for the two others, we get three terms that are each bounded using (3a), concluding the proof of (3b). □

Rounding to a classical strategy: Order the questions in Q such that $\pi(q_1)\geq\pi(q_2)\geq\ldots\geq\pi(q_n)$. Define a joint distribution on answers $a_1,\ldots,a_n$ as

$$D(a_1,\ldots,a_n)=\|(W^{a_n}_{q_n}\cdots W^{a_1}_{q_1}\otimes\mathrm{Id})|\Psi\rangle\|^2.$$

Fact 13 shows that D is a probability distribution, $\sum_{a_1,\ldots,a_n}D(a_1,\ldots,a_n)=1$.

We can interpret the distribution D as follows: Before the game starts, the provers produce a joint list of answers $a_1, \ldots, a_n$ as follows: They take the first part of $|\Psi\rangle$ and perform the projective measurement corresponding to question q_1. They obtain an outcome a_1, which they record. They then take the post-measurement state and perform on it the measurement corresponding to question q_2, and so on, each time using the post-measurement state of one measurement as the input state of the next measurement. The probability that the provers record answers $a_1, \ldots, a_n$ is precisely $D(a_1, \ldots, a_n)$.

Obviously neither quantum states nor measurements are needed to implement this constructed classical strategy. Before the game starts, the provers simply compute D for all inputs and sample from D using their shared randomness. When presented with questions q_i, q_j they give the answer a_i, a_j, ignoring all other answers in their sample. Hence the probability to answer a_i, a_j in this case is given by the marginal of D with respect to a_i and a_j, which we denote by $p_{class}(a_i a_j | q_i q_j)$.

Lemma 15. *The (weighted) statistical distance between p_{class} and p_q is*

$$\Delta(p_{class}, p_q) = \sum_{q,q'} \pi(q,q') \sum_{a,a'} |p_{class}(a,a'|q,q') - p_q(a,a'|q,q')| \leq 70 \cdot |Q| \cdot \varepsilon^{1/4}.$$

Let us first show how this proves Lemma 11. Since the quantum strategy of the provers passes the classical test with probability at least $1 - 6\varepsilon$, this means that the classical strategy wins the original game with probability at least $1 - 6\varepsilon - \Delta(p_{class}, p_q)$ (where Δ is the dominating term), which we want to be larger than s. This is achieved for $\varepsilon = \frac{s_q}{|Q|^4}$ for a sufficiently small constant s_q. □

Proof of Lemma 15. Let q_i, q_j be two questions. For convenience, let us introduce the notation $\sum_{\mathbf{a}}$ to denote summing over $a_1, \ldots, a_n$ and $\sum_{\mathbf{a}_{\neg i,j}}$ to denote summing over all $a_1, \ldots, a_n$ except a_i and a_j. Then the probability of answering (a_i, a_j) to (q_i, q_j) is $p_{class}(a_i a_j | q_i q_j) = \sum_{\mathbf{a}_{\neg i,j}} \|(W_{q_n}^{a_n} \cdots W_{q_1}^{a_1} \otimes \mathrm{Id}\,)|\Psi\rangle\|^2$ in the classical strategy, and $p_q(a_i, a_j | q_i, q_j) = \|W_{q_i}^{a_i} \otimes W_{q_j}^{a_j} |\Psi\rangle\|^2$ in the quantum strategy. We wish to bound

$$\sum_{a_i, a_j} \big| p_{class}(a_i a_j | q_i q_j) - p_q(a_i, a_j | q_i, q_j) \big| = \sum_{a_i, a_j} \big| \sum_{\mathbf{a}_{\neg i,j}} \|(W_{q_n}^{a_n} \cdots W_{q_1}^{a_1} \otimes \mathrm{Id}\,)|\Psi\rangle\|^2 - \|W_{q_i}^{a_i} \otimes W_{q_j}^{a_j} |\Psi\rangle\|^2 \big|.$$

We now use a hybrid argument to go from the classical to the quantum probability. The point is to eliminate the excess W_q^a in p_{class} with the help of Fact 13, which allows to eliminate a sum over a that involves a W_q^a on the *left* side of all other operators in $\|\cdot\|^2$. To get all unwanted W_q^a to be on the left, we move matrices from one register to the other whenever they are on the *right*, closest to $|\Psi\rangle$, at the expense of some error which we can bound using Eqs.(3). More precisely we use the triangle inequality for matrices A, W, B, W'

$$\big| \|(AW \otimes BW')|\Psi\rangle\| - \|(AW' \otimes BW)|\Psi\rangle\| \big| \leq \|(A \otimes B)[W \otimes W' - W' \otimes W]|\Psi\rangle\|, \tag{4}$$

where A and B will be sequences of W_q^a and W or W' are either one of the W_q^a or the identity.

To describe the sequence along which we move the matrices around, let us use the shorthand notation W_k for $W_{q_k}^{a_k}$. At each step we will interchange either $W_k \otimes \mathrm{Id} \leftrightarrow \mathrm{Id} \otimes W_k$ or $W_i \otimes W_k \leftrightarrow W_k \otimes W_i$ whenever they are on the right. If $i > j$ we proceed according to the sequence

$$\begin{aligned}
&W_n \cdots W_1 \otimes \mathrm{Id} \to W_n \cdots W_2 \otimes W_1 \to W_n \cdots W_3 \otimes W_1 W_2 \to \cdots \to W_n \cdots W_{i+1} W_i \otimes W_1 \cdots W_{i-1} \\
&\to W_n \cdots W_{i+1} W_{i-1} \otimes W_1 \cdots W_{i-2} W_i \to W_n \cdots W_{i+1} W_{i-1} W_i \otimes W_1 \cdots W_{i-2} \\
&\to W_n \cdots W_{i+1} W_{i-1} W_{i-2} \otimes W_1 \cdots W_{i-3} W_i \to \cdots \to W_n \cdots W_{i+1} W_{i-1} \cdots W_{j+1} W_i \otimes W_1 \cdots W_j.
\end{aligned}$$

Note that the last term in the sequence, when summed over $\mathbf{a}_{\neg i,j}$, equals $p_q(a_i a_j | q_i q_j)$ because of Fact 13, i.e. $\sum_{\mathbf{a}_{\neg i,j}} \|W_n \cdots W_{j+1} W_i \otimes W_1 \cdots W_j |\Psi\rangle\|^2 = \|W_i \otimes W_j |\Psi\rangle\|^2 = p_q(a_i a_j | q_i q_j)$. Now we can write a

telescopic sum according to this sequence as

$$\sum_{a_i,a_j} |p_{class}(a_ia_j|q_iq_j) - p_q(a_ia_j|q_iq_j)| = \sum_{a_i,a_j} \Big| \sum_{\mathbf{a}_{\neg i,j}} \|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\|^2 - \sum_{\mathbf{a}_{\neg i,j}} \|W_n \cdots W_2 \otimes W_1|\Psi\rangle\|^2 + \sum_{\mathbf{a}_{\neg i,j}} \|W_n \cdots W_2 \otimes W_1|\Psi\rangle\|^2 - \sum_{\mathbf{a}_{\neg i,j}} \|W_n \cdots W_3 \otimes W_1W_2|\Psi\rangle\|^2 + \cdots \Big|$$
$$\leq \sum_{\mathbf{a}} \big| \|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\|^2 - \|W_n \cdots W_2 \otimes W_1|\Psi\rangle\|^2 \big| + \sum_{\mathbf{a}} \big| \cdots \big| + \cdots,$$

where we used the triangle inequality. Using $|a^2 - b^2| = |a-b| \cdot |a+b|$, and the triangle inequality as in (4), the first term is bounded by

$$\sum_{\mathbf{a}} \|W_n \cdots W_2[W_1 \otimes \mathrm{Id} - \mathrm{Id} \otimes W_1]|\Psi\rangle\| \cdot (\|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\| + \|W_n \cdots W_2 \otimes W_1|\Psi\rangle\|)$$
$$\leq \sqrt{\sum_{\mathbf{a}} \|W_n \cdots W_2[W_1 \otimes \mathrm{Id} - \mathrm{Id} \otimes W_1]|\Psi\rangle\|^2} \sqrt{\sum_{\mathbf{a}} (\|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\| + \|W_n \cdots W_2 \otimes W_1|\Psi\rangle\|)^2},$$

where we used Cauchy-Schwarz for the inequality. We obtain similar expressions for all other terms. We can bound the second square root by $\sqrt{2+2} = 2$, using $(a+b)^2 \leq 2a^2 + 2b^2$ and Fact 13. Assembling all the terms, and using Fact 13 to eliminate all the matrices to the left of the square brackets, we obtain

$$\sum_{a_i,a_j} |p_{class}(a_ia_j|q_iq_j) - p_q(a_ia_j|q_iq_j)| \leq 2 \sum_{i'=1}^{i-1} \sqrt{\sum_{a_{i'}} \|[W_{i'} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{i'}]|\Psi\rangle\|^2}$$
$$+ 2(|i-j|+1) \sqrt{\sum_{a_i} \|[\mathrm{Id} \otimes W_i - W_i \otimes \mathrm{Id}\,]|\Psi\rangle\|^2}$$
$$+ 2 \sum_{i'=j+1}^{i-1} \sqrt{\sum_{a_i,a_{i'}} \|[W_i \otimes W_{i'} - W_{i'} \otimes W_i]|\Psi\rangle\|^2}. \qquad (5)$$

For $j > i$ we obtain exactly the same sequence and the same bounds in Eq. (5) with i and j interchanged. The only difference is that now the last term in the sequence, when summed over $\mathbf{a}_{\neg i,j}$ gives $\|W_j \otimes W_i|\Psi\rangle\|^2$, so we need to use symmetry of $|\Psi\rangle$ to conclude that this equals to $\|W_i \otimes W_j|\Psi\rangle\|^2$. For $i = j$ we follow the sequence until $W_n \cdots W_{i+1}W_i \otimes W_1 \cdots W_{i-1}$ and then use $W_i = W_i^2$ to continue as $W_n \cdots W_{i+1}W_iW_i \otimes W_1 \cdots W_{i-1} \to W_n \cdots W_i \otimes W_1 \cdots W_{i-1}W_i$, so we just get the first term in Eq. (5), but summed until i.

Now $\Delta(p_{class}, p_q)$ is bounded by the average over (q_i, q_j) picked according to the distribution π of the sum of the three terms appearing in (5). We show how to bound each of them. For the first term

$$2 \sum_{i,j=1}^{|Q|} \pi(q_i,q_j) \sum_{i'=1}^{i} \sqrt{\sum_{a_{i'}} \|(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}})|\Psi\rangle\|^2}$$
$$= 2 \sum_{i=1}^{|Q|} \pi(q_i) \sum_{i'=1}^{i} \sqrt{\sum_{a_{i'}} \|(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}})|\Psi\rangle\|^2}$$
$$\leq 2 \sum_{i=1}^{|Q|} \sum_{i'=1}^{|Q|} \pi(q_{i'}) \sqrt{\sum_{a_{i'}} \|(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}})|\Psi\rangle\|^2}$$
$$\leq 2|Q| \Big(\sum_{i'=1}^{|Q|} \pi(q_{i'}) \sum_{a_{i'}} \|(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}})|\Psi\rangle\|^2 \Big)^{1/2} \leq 2|Q|\sqrt{9 \cdot 24\varepsilon},$$

where the first equality uses the fact that the inner sum does not depend on j, the second inequality uses $\pi(q_i) \leq \pi(q_{i'})$, the third inequality uses the fact that the square of the expectation is not greater than the expectation of the square, and the last inequality uses Eq. (3b). The second term can be bounded in a similar fashion

$$2\sum_{i,j=1}^{|Q|}\pi(q_i,q_j)(|i-j|+1)\sqrt{\sum_{a_i}\|(\mathrm{Id}\otimes W_{q_i}^{a_i}-W_{q_i}^{a_i}\otimes\mathrm{Id})|\Psi\rangle\|^2}$$
$$\leq 2|Q|\sum_{i=1}^{|Q|}\pi(q_i)\sqrt{\sum_{a_i}\|(\mathrm{Id}\otimes W_{q_i}^{a_i}-W_{q_i}^{a_i}\otimes\mathrm{Id})|\Psi\rangle\|^2}\leq 2|Q|\sqrt{9\cdot 24\varepsilon}.$$

Finally the last term, using again that the inner sum does not depend on j, that the square of the expectation is bounded by the expectation of the square and Cauchy-Schwarz for the sum over i', can be bounded by

$$2\sum_{i=1}^{|Q|}\pi(q_i)\sum_{i'=1}^{i-1}\sqrt{\sum_{a_i,a_{i'}}\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2}$$
$$\leq 2\Big(\sum_{i=1}^{|Q|}\pi(q_i)\Big(\sum_{i'=1}^{i-1}\sqrt{\sum_{a_i,a_{i'}}\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2}\ \Big)^2\Big)^{1/2}$$
$$\leq 2\sqrt{|Q|}\Big(\sum_{i=1}^{|Q|}\pi(q_i)\sum_{i'=1}^{i-1}\sum_{a_i,a_{i'}}\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2\Big)^{1/2}. \tag{6}$$

We decompose the sum inside the square root in the last line of (6) into two parts with $\pi(q_i)\geq 1/h$ and $\pi(q_i)<1/h$ (with h to be determined later). If $\pi(q_i)\geq 1/h$, then $\pi(q_{i'})\geq 1/h$ for $i'\leq i$ so $1\leq h\pi(q_{i'})$. Therefore, using (3a), the term in parenthesis in (6) is bounded by

$$\sum_{i:\pi(q_i)\geq 1/h}\sum_{i'=1}^{i-1}h\pi(q_{i'})\pi(q_i)\sum_{a_i,a_{i'}}\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2$$
$$+\frac{1}{h}\sum_{i:\pi(q_i)\leq 1/h}\sum_{i'=1}^{i-1}\sum_{a_i,a_{i'}}\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2\leq 24h\varepsilon+4|Q|^2/h,$$

where we have bounded the first part using (3a) and the second part, using triangle inequality and Fact 13

$$\sum_{a_i,a_{i'}}\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2\leq\sum_{a_i,a_{i'}}(\|(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}})|\Psi\rangle\|+\|(W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i})|\Psi\rangle\|)^2\leq 4.$$

The optimal h is $|Q|/\sqrt{6\varepsilon}$, which gives a bound of $4\cdot 24^{1/4}|Q|\varepsilon^{1/4}$ for the third (dominant) term in $\Delta(p_{class},p_q)$ (after taking the square root). Hence $\Delta(p_{class},p_q)\leq 70|Q|\varepsilon^{1/4}$. □

4 Hardness of three-prover entangled classical games

In this section we prove Theorem 1 for three-prover entangled classical games, which we now state as:

Theorem 16. *There is a constant $s_3>0$ such that it is* NP*-hard to decide, given an entangled three-prover classical game with a constant number of answers, whether its value is* 1 *or less than* $1-\varepsilon$ *for* $\varepsilon=\frac{s_3}{|Q|^2}$.

As in the case of quantum games, we will prove this by a reduction from the PCP Theorem. This time, however, we will essentially preserve the number of answers in the modified game.

We begin by describing how to modify any two-prover classical game $G(2, \pi, V)$ (which is assumed to be symmetric per Lemma 4) to a three-prover classical game G' of equal or higher value.

The modified three-prover game. In the constructed game G' the verifier chooses one of the provers uniformly at random. Rename the chosen prover Alice and call the other provers Bob and Cleve. The verifier samples questions q and q' according to $\pi(q, q')$. He sends question q to Alice, and question q' to both Bob and Cleve. He receives answers a, a', and a'', respectively, and accepts iff the following are both true:

Classical Test: The answers of Alice and Bob would win the game G, i.e., $V(aa'|qq') = 1$.

Consistency: Bob and Cleve give the same answer, i.e., $a' = a''$.

Remarks: Note that unlike the quantum case, the verifier performs both tests at the same time. The consistency test plays the role of the SWAP test, limiting the advantage gained by sharing entanglement.

Again it is clear that the value of the constructed game is at least as large as the value of the original game G: if the provers reply according to an optimal classical strategy (which can be assumed to be symmetric per Lemma 4) they always pass the consistency-test. Also, it is clear in this case that the size of the description of the constructed game is linearly related to the size of the description of the original game, hence we have the same complexity parameter.

To prove Theorem 16, we need to show the following.

Lemma 17. *If $\omega^*(G') > 1 - \varepsilon$ then $\omega(G) > s$.*

Proof. Consider a quantum strategy for G' that succeeds with probability $1 - \varepsilon$.[16] Since the game G' is symmetric, we can assume that this strategy is symmetric, per Lemma 5. Suppose that the provers share a symmetric state $|\Psi\rangle \in \mathcal{H}^{\otimes 3}$. Let $\rho^{\mathrm{AB}} = \mathrm{tr}_{\mathcal{H}_3} |\Psi\rangle\langle\Psi|$ be the reduced density matrix of $|\Psi\rangle\langle\Psi|$ on Alice and Bob. When asked question q_i, each prover measures their part of $|\Psi\rangle$. Following standard arguments (extending the private space of the provers) we can assume that this measurement is projective. Let $W_{q_i}^{a_i}$ be the projector corresponding to question q_i and answer a_i. This defines the quantum strategy for G'; it passes the classical test with probability

$$\pi_1 = \sum_{aa'qq'} \pi(q, q') V(aa'|qq') p_q(aa'|qq'),$$

where

$$p_q(aa'|qq') = \mathrm{tr}\left(W_q^a \otimes W_{q'}^{a'} \rho^{\mathrm{AB}}\right) = \langle\Psi| W_q^a \otimes W_{q'}^{a'} \otimes \mathrm{Id}\ |\Psi\rangle. \tag{7}$$

It passes the consistency test with probability $\pi_2 = \sum_q \pi(q)\pi_2(q)$, where $\pi(q)$ is the marginal of $\pi(q, q')$ and

$$\pi_2(q) = \sum_a \mathrm{tr}\left(W_q^a \otimes W_q^a \rho^{\mathrm{AB}}\right) = \sum_a \langle\Psi| W_q^a \otimes W_q^a \otimes \mathrm{Id}\ |\Psi\rangle, \tag{8}$$

where we made use of the symmetry. Note that $\pi_1, \pi_2 \geq 1 - \varepsilon$.

Eqs. (7) and (8) clarify the role of the third prover, Cleve. His main purpose is *not* to allow the two tests to be performed at the same time: Indeed, it is possible to modify the protocol so that the verifier chooses two

[16] Again, as in Section 3.2, we in fact consider a strategy with finite entanglement that has success probability $1 - \varepsilon - \delta$ for some $\delta = O(\varepsilon)$, which we will not write.

of the provers at random (say Alice and Bob) and only sends questions to them, not interacting with the third prover at all.[17] Cleve's presence would not be important if the provers were executing a classical strategy, but it can (and does) make a difference if their strategy requires entanglement. Indeed, if there were only two provers, then they could share any state ρ^{AB}, whereas here we require that ρ^{AB} be *extendable*, i.e., it must be the reduced density matrix of a symmetric tripartite state. To give a concrete example, it is not possible for ρ^{AB} to be the maximally entangled state $|\Psi^-\rangle\langle\Psi^-|$. This is termed *monogamy of entanglement* [Wer89].

Rounding to a classical strategy: We construct a classical strategy for G from the quantum strategy for G' in a similar fashion as in the case of quantum games, with

$$D(a_1, \ldots, a_n, a'_1, \ldots, a'_n) = \|W^{a_n}_{q_n} \cdots W^{a_1}_{q_1} \otimes W^{a'_n}_{q_n} \cdots W^{a'_1}_{q_1} \otimes \mathrm{Id}\ |\Psi\rangle\|^2. \tag{9}$$

where $q_1, \ldots, q_n$ is an ordering of the questions in Q such that $\pi(q_1) \geq \pi(q_2) \geq \ldots \geq \pi(q_n)$.[18] As before, we define $p_{class}(a_i, a'_j|q_i, q_j)$ to be the marginal of D on a_i, a'_j. The structure of our proof that this strategy is a good one is very similar to the quantum case. The details, however, are a little different.

Lemma 18. *The (weighted) statistical distance between p_{class} and p_q is*

$$\Delta(p_{class}, p_q) = \sum_{q,q'} \pi(q, q') \sum_{a,a'} |p_{class}(a, a'|q, q') - p_q(a, a'|q, q')| \leq 12|Q|\sqrt{\varepsilon}.$$

We first show how this Lemma proves Lemma 17. Since the strategy in the entangled game passes the classical test with probability at least $1 - \varepsilon$, the classical strategy succeeds in the original game with probability at least $1 - \varepsilon - \Delta \geq 1 - \varepsilon - 12|Q|\sqrt{\varepsilon}$. For $\varepsilon = \frac{s_3}{|Q|^2}$ for sufficiently small constant s_3, this probability is larger than s. □

This Lemma is the corresponding version of Lemma 15. Why is it true? Rather than showing that the order of measurements is not important as we did in the quantum case (although it will turn out in hindsight that this is true), we show that each measurement does not disturb ρ^{AB} very much. The key observation is as follows. Assume the provers pass the consistency test with high probability. If a particular measurement result occurs with certainty, the quantum state cannot be changed by the measurement. We use this fact in the following way: suppose Cleve were to perform the measurement corresponding to question q and assume he obtains an outcome a. Then, if Bob is asked question q, he must also give answer a with high probability. So his measurement does not change the quantum state much. But, since quantum theory is no-signalling, it cannot matter who measured first. It follows that Bob's measurement does not change ρ^{AB} much. Note that only the bipartite state ρ^{AB} is approximately unchanged—Bob's measurement can change the tri-parite state $|\Psi\rangle\langle\Psi|$ considerably. We then use a hybrid argument to show that performing all the measurements one after the other also leaves ρ^{AB} approximately unchanged. This part of the proof mirrors the proof of Lemma 15.

Proof of Lemma 18. Let $\mathcal{W}_q$ be the superoperator corresponding to the projective measurement q, i.e., $\mathcal{W}_q(\sigma) := \sum_a W^a_q \sigma (W^a_q)^\dagger$ is the post-measurement state after performing $\{W^a_q\}$ on state σ.

To quantify how much a measurement changes a state we use Winter's gentle measurement lemma.

Lemma 19 (Lemma I.4 [Win99])**.** *Let ρ be a state and X be a positive matrix with $X \leq \mathrm{Id}$ and $0 \leq \mathrm{Tr}\rho X$. Then,*

$$\left\| \rho - \sqrt{X}\rho\sqrt{X} \right\|_1 \leq 3\sqrt{1 - \mathrm{Tr}X\rho}.$$

[17] With probability p, he sends them different questions and performs the classical test; with probability $1 - p$, he sends the same question and performs the consistency test—this modification does not materially change our conclusions, but it does weaken the bounds in Theorem 16.

[18] Note that D differs slightly from Sec. 3.2. Here each prover gets a separate list of answers. This form is more convenient here.

The following simple corollary quantifies how much the measurement $\mathcal{W}_q \otimes \mathrm{Id}$ changes ρ^{AB}:

Claim 20. *The trace distance between $\mathcal{W}_q \otimes \mathrm{Id}\,(\rho^{AB})$ and ρ^{AB} is bounded by*

$$\|\mathcal{W}_q \otimes \mathrm{Id}\,(\rho^{AB}) - \rho^{AB}\|_1 \leq 6\sqrt{1-\pi_2(q)}.$$

Proof. Using $\mathcal{W}_q \otimes \mathrm{Id}\,(\rho^{\mathrm{AB}}) = \mathrm{tr}_{\mathcal{H}_3}(\mathcal{W}_q \otimes \mathrm{Id} \otimes \mathrm{Id}\,(|\Psi\rangle\langle\Psi|))$ and $\rho^{\mathrm{AB}} = \mathrm{tr}_{\mathcal{H}_3}(\mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|))$, by monotonicity of the trace distance under partial trace,

$$\begin{aligned}
\|\mathcal{W}_q \otimes \mathrm{Id}\,(\rho^{\mathrm{AB}}) - \rho^{\mathrm{AB}}\|_1 &\leq \|\mathcal{W}_q \otimes \mathrm{Id} \otimes \mathrm{Id}\,(|\Psi\rangle\langle\Psi|) - \mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|)\|_1 \\
&\leq \|\mathcal{W}_q \otimes \mathrm{Id} \otimes \mathrm{Id}\,(|\Psi\rangle\langle\Psi|) - \sum_a W_q^a \otimes \mathrm{Id} \otimes W_q^a |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes W_q^a\|_1 \\
&\quad + \|\sum_a W_q^a \otimes \mathrm{Id} \otimes W_q^a |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes W_q^a - \mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|)\|_1 \\
&\leq 2\|\sum_a W_q^a \otimes \mathrm{Id} \otimes W_q^a |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes W_q^a - \mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|)\|_1 \\
&\leq 6\sqrt{1-\pi_2(q)},
\end{aligned}$$

by the triangle inequality, symmetry, and then taking $\rho = \bigoplus_a W_q^a \otimes \mathrm{Id} \otimes \mathrm{Id}\ |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes \mathrm{Id}$ and $X = \bigoplus_a \mathrm{Id} \otimes \mathrm{Id} \otimes W_q^a$ in Lemma 19. □

For $1 \leq i, j \leq n$, let

$$\rho^{\mathrm{AB}}(i,j) := (\mathcal{W}_{q_{i-1}} \circ \cdots \circ \mathcal{W}_{q_1}) \otimes (\mathcal{W}_{q_{j-1}} \circ \cdots \circ \mathcal{W}_{q_1})\rho^{\mathrm{AB}}$$

Then

$$p_{class}(a_i a'_j | q_i q'_j) = \mathrm{tr}\left((W_{q_i}^{a_i} \otimes W_{q'_j}^{a'_j})\rho(i,j)\right)$$

Hence if we can bound $\|\rho(i,j) - \rho\|_1$, then we can bound $\sum_{a_i, a'_j} |p_{class}(a_i a'_j | q_i q'_j) - p_q(a_i a'_j | q_i q'_j)|$, since the trace distance between two states is an upper bound on the variation distance of the probability distribution resulting from making any measurement on those two states.

The following technique was introduced by Ambainis, Nayak, Ta-Shma, and U. Vazirani [ANTV02] and has been used extensively by Aaronson [Aar05, Aar06].

Claim 21. *The trace distance between $\rho^{AB}(i,j)$ and ρ^{AB} is bounded by*

$$\|\rho^{AB}(i,j) - \rho^{AB}\|_1 \leq 6\sum_{i'=1}^{i-1} \sqrt{1-\pi_2(q_{i'})} + 6\sum_{j'=1}^{j-1} \sqrt{1-\pi_2(q_{j'})}.$$

Proof. Proof by induction. The claim is clearly true for $(i,j) = (1,1)$. Given it is true for a particular value of (i,j), we show it is also true for $(i+1,j)$. In view of the symmetry, this is sufficient to establish the claim. We have

$$\begin{aligned}
\|\rho^{\mathrm{AB}}(i+1,j) - \rho^{\mathrm{AB}}\|_1 &\leq \|\rho^{\mathrm{AB}}(i+1,j) - \mathcal{W}_{q_i} \otimes \mathrm{Id}\,(\rho^{\mathrm{AB}})\|_1 + \|\mathcal{W}_{q_i} \otimes \mathrm{Id}\,(\rho^{\mathrm{AB}}) - \rho^{\mathrm{AB}}\|_1 \\
&\leq \|\mathcal{W}_{q_i} \otimes \mathrm{Id}\ \left(\rho^{\mathrm{AB}}(i,j) - \rho^{\mathrm{AB}}\right)\|_1 + 6\sqrt{1-\pi_2(q_i)} \\
&\leq \|\rho^{\mathrm{AB}}(i,j) - \rho^{\mathrm{AB}}\|_1 + 6\sqrt{1-\pi_2(q_i)},
\end{aligned}$$

where we used the triangle inequality, Claim 20, and monotonicity of the trace distance. □

Putting everything together, it follows that

$$\begin{aligned}
\Delta(p_{class}, p_q) &\leq \sum_{i,j=1}^{n} \pi(q_i, q'_j) \|\rho^{\mathrm{AB}}(i,j) - \rho^{\mathrm{AB}}\|_1 \\
&\leq 6 \sum_{i,j=1}^{n} \pi(q_i, q'_j) \left(\sum_{i'=1}^{i-1} \sqrt{1 - \pi_2(q_{i'})} + \sum_{j'=1}^{j-1} \sqrt{1 - \pi_2(q_{j'})} \right) \\
&\leq 12 \sum_{i=1}^{n} \sum_{i'=1}^{i-1} \pi(q_i) \sqrt{1 - \pi_2(q_{i'})} \\
&\leq 12|Q| \sum_{i'=1}^{n} \pi(q_{i'}) \sqrt{1 - \pi_2(q_{i'})} \\
&\leq 12|Q| \sqrt{1 - \pi_2} \leq 12|Q|\sqrt{\epsilon},
\end{aligned}$$

since $\pi_2 = \sum_q \pi(q)\pi_2(q) \geq 1 - \varepsilon$ and $\sqrt{1-x}$ is concave. □

5 Hardness for two-prover classical entangled games

In this section we prove our main theorem for two-prover entangled classical games. It shows that it is PSPACE-hard to decide, given a succinct entangled two-prover classical game, whether its value is 1 or less than $1 - \varepsilon$ for $\varepsilon = \frac{1}{\mathrm{poly}(|x|)}$. To state the result, we need some further definitions to clarify the notion of succinctly given games and state the connection between PSPACE and multi-round single-prover games.

Definition 22. *A language L is in $\mathrm{MIP}^*_{c,s}(N, 1)$ if, for all $x \in L$, there is a polynomial time (in $|x|$) mapping from x to classical one-round games $G_x(N, \pi_x, V_x)$, such that it is possible to sample from π_x in polynomial time and compute the predicate V_x in polynomial time and*

- *Completeness: for all $x \in L$, the entangled value $\omega^*(G_x) \geq c$, and*
- *Soundness: for all $x \notin L$, the entangled value $\omega^*(G_x) \leq s$.*

Note that in this scenario the game is given *succinctly*: it is given by a description of V (as a polynomial time circuit, for instance, which implies that $|Q|, |A| = 2^{\mathrm{poly}(|x|)}$) and a polynomial size description of π, which can be sampled in polynomial time. Hence the complexity parameter here is $|x|$, and $|Q|$ and $|A|$ are exponential.

We also require the notion of single-prover games with multiple rounds. We modify Definition 3 to account for games with multiple rounds. Here we will only consider *non-adaptive* games: the probability distribution on questions in Q for each round k does not depend on the answers received in previous rounds, which is sufficient for PSPACE (see Theorem 23). However, we allow for the possibility that the questions asked in each round depend on the questions asked in previous rounds.[19] In other words a one-player r-round game $G(1, \pi_r, V_r)$ is given by a joint distribution $\pi : Q^r \to [0, 1]$, and a predicate $V_r : A^r \times Q^r \to \{0, 1\}$ (i.e. the verifier accepts or rejects as a function of all the answers received in all rounds). The strategy is now a set of r functions W_k, where the kth function can depend on the previous questions and answers. The class $\mathrm{IP}(r)$ is given by Definition 22 when the game is a single-prover multi-round game with r rounds. We omit reference to r and write IP when the number of rounds is polynomial in $|x|$.

[19] Note that this is equivalent to having a joint distribution on the questions, where we obtain the distribution on the ith question as the corresponding marginal.

Theorem 23. *[Sha92] There is a constant $s_{IP} \geq 0$ such that* PSPACE $=$ IP$_{1,s_{IP}}$. *Moreover there are "public-coin non-adaptive"* IP*-protocols for* PSPACE*, i.e. such that in each round the distribution on the questions is independent of the answers of the prover and of other rounds [GS89, She92].*

With these notions in place we can state our main result for two-prover classical entangled games.

Theorem 24. PSPACE $\subseteq$ MIP$^*(2,1)_{1,1-\varepsilon}$ *for* $\varepsilon = \frac{1}{\mathrm{poly}(|x|)}$*, where* $|x|$ *is the input size.*

We note that if a parallel repetition theorem could be established for classical two-prover entangled games, then the containment in Theorem 24 could be improved to PSPACE $\subseteq$ MIP$^*(2,1)_{1,s}$ with constant or even exponentially small s. This is a particularly interesting direction to pursue, in light of the perfect parallel repetition theorem for entangled XOR games of Cleve et al. [CSUU07] (which uses the SDP-description on the value of these games).

To prove Theorem 24 we use the PSPACE-characterization in Theorem 23 and show the following.

Lemma 25. *There is a constant $s_2 \geq 0$ such that for every succinctly given single-prover r-round non-adaptive game $G(1, \pi_r, V_r)$, of value $\omega(G)$ with questions Q and answers A, there is a two-prover one-round classical game $G_c(2, \pi, V)$ with questions Q^r and answers A^r with entangled value $\omega^*(G_c) \geq \omega(G)$ such that if $\omega^*(G_c) > 1 - \varepsilon$ then $\omega(G) > s_{IP}$ for $\varepsilon = \frac{s_2}{r^2}$. Moreover, a succinct description of G_c can be computed from a description of G in polynomial time, and sampling π and computing V can be done in polynomial time.*

Lemma 25 shows IP$(r)_{1,s_{IP}} \subseteq$ MIP$(2,1)^*_{1,1-\frac{s_2}{r^2}}$, and combined with Theorem 23 gives Theorem 24.

The rest of this section is dedicated to the proof of Lemma 25. It follows the main traits of the proofs of the previous two hardness results. Our construction of the two-prover one-round game uses a protocol of [CCL94] used to prove that PSPACE has two-prover one-round systems. We show that this protocol remains sound even against entangled provers, albeit with larger soundness. To prove this we again use the consistency test with the extra prover to extract almost commuting conditions on the operators of the provers. This allows us to round in a similar fashion from a good strategy for the entangled game to a strategy for the single prover game which succeeds with relatively large probability.

The modified two-prover game. In the constructed game G_c, the verifier samples a series of questions $q_1, \ldots, q_r$ according to the distribution $\pi_r(q_1, \ldots, q_r)$. He picks a k uniformly at random in $\{1, \ldots, r\}$, and sends questions $q_1, q_2, \ldots, q_r$ to Alice and $q_1, q_2, \ldots, q_k$ to Bob. He receives answers $a = a_1, \ldots, a_r$ from Alice and $a' = a'_1, \ldots, a'_k$ from Bob. He accepts if and only if the following are both true:

Classical Test The answers Alice gives would win the game G: $V(a_1 \ldots a_n | q_1 \ldots q_n) = 1$.

Consistency Test For all i in $\{1, \ldots, k\}$, $a_i = a'_i$.

Remark: It is again obvious that the value of the new game is lower bounded by the value of the original game: If both provers reply according to an optimal classical strategy, then they will always give consistent answers, so their acceptance probability is exactly $\omega(G)$.

It is also easy to see that the constructed game has the same complexity as the original game. The new verifier essentially implements the original verifier and the consistency test, which can be described in linear time in A^r. The sampling procedure also has the same complexity as sampling from the original π_r. And obviously it is possible to compute the new game from the original game in polynomial time.

To prove Lemma 25 we need to show the following.

Lemma 26. *If $\omega^*(G_c) > 1 - \varepsilon$ then $\omega(G) > s_{IP}$.*

Proof. Consider a quantum strategy for G' that succeeds with probability $1-\varepsilon$.[20] For any sequence of questions $q_1,\ldots,q_r$ we define $\mathbf{q}_k$ to be the sequence $q_1,\ldots,q_k$. Similarly, for any sequence $a=a_1,\ldots,a_r$ of possible answers we will denote its prefix $a_1,\ldots,a_k$ by $\mathbf{a}_k$. Note that when we write $\mathbf{a}_k$ and $\mathbf{a}_l$ for some $1\leq k,l\leq r$ we refer to substrings of the *same* string $a=a_1,\ldots,a_r$, whereas we will write $\mathbf{a}_k$ and $\mathbf{a}'_l$ if we refer to *different* strings a and a'.

Let $|\Psi\rangle$ be the entangled state shared by Alice and Bob and define a corresponding density matrix $\rho=|\Psi\rangle\langle\Psi|$. Let $\tilde{\mathcal{W}}_{\mathbf{q}_r}=\{\tilde{W}^{\mathbf{a}_r}_{\mathbf{q}_r}\}$ and $\mathcal{W}_{\mathbf{q}_r}=\{W^{\mathbf{a}'_k}_{\mathbf{q}_k}\}$ be the measurements that they perform when asked questions $\mathbf{q}_r$ resp. $\mathbf{q}_k$ giving answers $\mathbf{a}_r$ resp. $\mathbf{a}'_k$. As in Sec. 4 we can assume that these measurements are projective.

The provers pass the consistency test with probability $\pi_2=\frac{1}{r}\sum_{k=1}^r\pi_2(k)$, where

$$\pi_2(k)=E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r}\mathrm{Tr}\left(\tilde{W}^{\mathbf{a}_r}_{\mathbf{q}_r}\otimes W^{\mathbf{a}_k}_{\mathbf{q}_k}\rho\right)\right]$$

is the probability that the two provers give consistent answers when the verifier has picked k as the separation point. Conditioned on the fact that they gave consistent answers, they succeed in the classical test with probability $\pi_1=\frac{1}{r}\sum_{k=1}^r\pi_1(k)$ where

$$\pi_1(k)=E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r}p_q(\mathbf{a}_r|\mathbf{q}_r,k)V(\mathbf{a}_r|\mathbf{q}_r)\right]$$

and $p_q(\mathbf{a}_r|\mathbf{q}_r,k)=\mathrm{Tr}\left(\tilde{W}^{\mathbf{a}_r}_{\mathbf{q}_r}\otimes W^{\mathbf{a}_k}_{\mathbf{q}_k}\rho\right)$ is the probability that Alice answers $\mathbf{a}_r$ and Bob answers consistently, given that the verifier picked index k.

Rounding to a classical strategy: Given a strategy for the constructed entangled-prover game G_c, we define a strategy for the classical prover of the original game G in the following way. In round k, given the questions to the prover so far are $\mathbf{q}_k$ and the prover gave answers $\mathbf{a}_{k-1}$, he answers a_k to question q_k with probability

$$p_{class}(a_k|\mathbf{q}_k,\mathbf{a}_{k-1})=\frac{\mathrm{Tr}\left(\mathrm{Id}\otimes W^{\mathbf{a}_k}_{\mathbf{q}_k}W^{\mathbf{a}_{k-1}}_{\mathbf{q}_{k-1}}\cdots W^{\mathbf{a}_1}_{\mathbf{q}_1}\rho\right)}{\mathrm{Tr}\left(\mathrm{Id}\otimes W^{\mathbf{a}_{k-1}}_{\mathbf{q}_{k-1}}\cdots W^{\mathbf{a}_1}_{\mathbf{q}_1}\rho\right)}$$

(recall that all $\mathbf{a}_k,\mathbf{a}_{k-1},\ldots,\mathbf{a}_1$ refer to substrings of the same string). Note that $\sum_{a_k}p_{class}(a_k|\mathbf{q}_k,\mathbf{a}_{k-1})$ could be less than 1 (we will see from its operational definition that it is always bounded by 1). To complete it to a probability distribution we add a special symbol "abort" that the prover can send in any round making him lose the game.[21]

This probability distribution has the following interpretation. For any operator A, denote $A(\rho)=A\rho A^\dagger$. In the first round the prover in the classical game receives a question q_1, and applies the measurement $\mathcal{W}_{\mathbf{q}_1}$ on Bob's part of ρ, answering a_1 with probability $\mathrm{Tr}\left(\mathrm{Id}\otimes W^{\mathbf{a}_1}_{\mathbf{q}_1}\rho\right)=p_{class}(\mathbf{a}_1|\mathbf{q}_1)$. He is then left with the state $\frac{\mathrm{Id}\otimes W^{\mathbf{a}_1}_{\mathbf{q}_1}(\rho)}{\mathrm{Tr}\left(\mathrm{Id}\otimes W^{\mathbf{a}_1}_{\mathbf{q}_1}\rho\right)}$. Upon receiving a question q_2 in the second round, he measures this state with $\mathcal{W}_{\mathbf{q}_2}$, answering a_2 with probability $\frac{\mathrm{Tr}\left(\mathrm{Id}\otimes W^{\mathbf{a}_2}_{\mathbf{q}_2}W^{\mathbf{a}_1}_{\mathbf{q}_1}\rho\right)}{\mathrm{Tr}\left(\mathrm{Id}\otimes W^{\mathbf{a}_1}_{\mathbf{q}_1}\rho\right)}=p_{class}(a_2|\mathbf{q}_2,\mathbf{a}_1)$ if as a result of his measurement he obtains a sequence $\mathbf{a}_2=a_1a_2$ consistent with the a_1 he had measured in the first round, and an abort

[20] Again, as in Section 3.2, we in fact consider a strategy with finite entanglement that has success probability $1-\varepsilon-\delta$ for some $\delta=O(\varepsilon)$, which we will not write.

[21] Technically speaking the extra symbol makes it a different game. We could also have the prover send a random answer whenever sampling from the complement of the distribution. This can at most increase the prover's winning probability, so both games have winning probability bounded by ω.

symbol in case the sequence he measures has an $a_1' \neq a_1$. The resulting state in case of non-abortion is $\frac{\mathrm{Id} \otimes W_{\mathbf{q}_2}^{\mathbf{a}_2} W_{\mathbf{q}_1}^{\mathbf{a}_1}(\rho)}{p_{class}(a_2|\mathbf{q}_2,\mathbf{a}_1)\mathrm{Tr}\left(\mathrm{Id} \otimes W_{\mathbf{q}_1}^{\mathbf{a}_1}\rho\right)} = \frac{\mathrm{Id} \otimes W_{\mathbf{q}_2}^{\mathbf{a}_2} W_{\mathbf{q}_1}^{\mathbf{a}_1}(\rho)}{\mathrm{Tr}\left(\mathrm{Id} \otimes W_{\mathbf{q}_2}^{\mathbf{a}_2} W_{\mathbf{q}_1}^{\mathbf{a}_1}\rho\right)}$. The prover proceeds similarly at the subsequent rounds. In other words the prover sequentially performs all the measurements $\mathcal{W}_{\mathbf{q}_k}$, and answers according to the resulting distribution, aborting in case the answers he measures in round k contradict the answers that he has already given in previous rounds.

What is the probability that a fixed sequence of answers $\mathbf{a}_r$ is given by the prover? We have that $p_{class}(\mathbf{a}_r|\mathbf{q}_r) = p_{class}(a_r|\mathbf{q}_r, \mathbf{a}_{r-1}) \cdot \cdots \cdot p_{class}(a_2|\mathbf{q}_2, a_1) \cdot p_{class}(a_1|\mathbf{q}_1)$. Because of cancellation, we obtain

$$p_{class}(\mathbf{a}_r|\mathbf{q}_r) = \mathrm{Tr}\left(\mathrm{Id} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_1}^{\mathbf{a}_1}\rho\right).$$

We will show that this classical strategy is a good one by relating $p_{class}(\mathbf{a}_r|\mathbf{q}_r)$ to $p_q(\mathbf{a}_r|\mathbf{q}_r, r)$ as per the following lemma.

Lemma 27. *The (weighted) statistical distance between p_{class} and p_q is*

$$\Delta(p_{class}, p_q) = E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r}\left|p_{class}(\mathbf{a}_r|\mathbf{q}_r) - p_q(\mathbf{a}_r|\mathbf{q}_r, r)\right|\right] \leq 7\,r\,\sqrt{\varepsilon}.$$

This lemma is the analogue of Lemmas 15 and 18, and its proof is very similar. Before proceeding to its proof, we first show how it implies Lemma 26. For the total acceptance probability of the entangled provers we have $1 - \varepsilon \leq 1/r \sum_{k=1}^{r} \min(\pi_1(k), \pi_2(k))$ because for any index k that is picked by the verifier, we require the provers to succeed in both the Classical Test and the Consistency Test. This implies that $\pi_1(r) \geq 1 - r\varepsilon$, so Bob's answers can be used to give correct answers to the Classical Test with probability at least $1 - r\varepsilon$, and by Lemma 27 this implies that the Classical Test has success probability at least $1 - r\varepsilon - 7r\sqrt{\varepsilon}$. For $\varepsilon = \frac{s_2}{r^2}$ for a sufficiently small constant s_2 this is more than s_{IP}, which implies Lemma 26. □

Proof of Lemma 27. As in the case of three-prover classical entangled games, the fact that Alice's and Bob's answers must be consistent means that Alice's answers can be used to predict Bob's, so Bob cannot use his share of the entanglement too much if they are to succeed in the Consistency Test. This means that the action of Bob's operators $\mathcal{W}$ on the entangled state ρ is close to the identity, at least when the first prover applies the corresponding $\tilde{\mathcal{W}}$ on his share of ρ. The following Claim makes this explicit and will be used to relate the classical and quantum strategies.

Claim 28. *Let the projector $\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} = \sum_{a_{k+1},\ldots,a_r} \tilde{W}_{\mathbf{q}_r}^{\mathbf{a}_r}$. The following hold for every $k \in \{1, \ldots, r\}$:*

$$E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_k}\left\|\mathrm{Id} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho)\right\|_1\right] \leq 3\sqrt{1 - \pi_2(k)}, \tag{10}$$

$$E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_k}\left\|\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes \mathrm{Id}\,(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho)\right\|_1\right] \leq 3\sqrt{1 - \pi_2(k)}, \tag{11}$$

$$E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_k}\left\|\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_{k-1}} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho)\right\|_1\right] \leq 1 - \pi_2(k). \tag{12}$$

Proof. Eqs. (10) and (11) are a direct application of Lemma 19, combined with the definition of $\pi_2(k)$. To

prove Eq. (12), note that since $\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_{k-1}} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho) \geq \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho)$, we have that

$$\begin{aligned}\left\| \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_{k-1}} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho) \right\|_1 &= \mathrm{Tr}(\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_{k-1}} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho)) - \mathrm{Tr}(\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_k} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k}(\rho)) \\ &= \sum_{a'_k \neq a_k, a'_{k+1}, \ldots, a'_r} \mathrm{Tr}(\tilde{W}_{\mathbf{q}_r}^{\mathbf{a}_{k-1} a'_k \ldots a'_r} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_k} \rho).\end{aligned}$$

Since $\sum_{\mathbf{a}_r, \mathbf{a}'_k} \mathrm{Tr}(\tilde{W}_{\mathbf{q}_r}^{\mathbf{a}_r} \otimes W_{\mathbf{q}_k}^{\mathbf{a}'_k} \rho) = 1$,

$$1 - \pi_2(k) = E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r, \mathbf{a}'_k \neq \mathbf{a}_k} \mathrm{Tr}(\tilde{W}_{\mathbf{q}_r}^{\mathbf{a}_r} \otimes W_{\mathbf{q}_k}^{\mathbf{a}'_k} \rho) \right] \geq E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r, a'_k \neq a_k} \mathrm{Tr}(\tilde{W}_{\mathbf{q}_r}^{\mathbf{a}_r} \otimes W_{\mathbf{q}_k}^{\mathbf{a}_{k-1}, a'_k} \rho) \right]$$

which concludes the proof. □

Observe that for any set of orthogonal projectors $\{W^a\}$ we have that $\sum_a \|W^a \sigma_1 W^a - W^a \sigma_2 W^a\|_1 \leq \|\sigma_1 - \sigma_2\|_1$ for any two matrices σ_1, σ_2. Using this successively for the sets $\{W_{\mathbf{q}_2}^{\mathbf{a}_2}\}_{a_2}$, ..., $\{W_{\mathbf{q}_r}^{\mathbf{a}_r}\}_{a_r}$, from Eq. (10) with $k = 1$ we get

$$E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r} \left\| \mathrm{Id} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_1}^{\mathbf{a}_1}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_1} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_1}^{\mathbf{a}_1}(\rho) \right\|_1 \right] \leq 3\sqrt{1 - \pi_2(1)}.$$

Similarly, from Eq. (11),

$$E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r} \left\| \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_1} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_1}^{\mathbf{a}_1}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_1} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_2}^{\mathbf{a}_2}(\rho) \right\|_1 \right] \leq 3\sqrt{1 - \pi_2(1)}$$

and from Eq. (12) with $k = 2$

$$E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r} \left\| \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_1} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_2}^{\mathbf{a}_2}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_2} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_2}^{\mathbf{a}_2}(\rho) \right\|_1 \right] \leq 1 - \pi_2(2)$$

Repeating these operations for each k, adding the equations and using triangle inequality finally yields

$$\begin{aligned}E_{\mathbf{q}_r}\left[\sum_{\mathbf{a}_r} \left\| \mathrm{Id} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r} \cdots W_{\mathbf{q}_1}^{\mathbf{a}_1}(\rho) - \tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_r} \otimes W_{\mathbf{q}_r}^{\mathbf{a}_r}(\rho) \right\|_1 \right] &\leq 6 \sum_{k=1}^{r} \sqrt{1 - \pi_2(k)} + \sum_{k=2}^{r} (1 - \pi_2(k)) \\ &\leq 7r\sqrt{1 - \pi_2}\end{aligned}$$

using concavity of the function $\sqrt{1-x}$. Since $\tilde{V}_{\mathbf{q}_r}^{\mathbf{a}_r} = \tilde{W}_{\mathbf{q}_r}^{\mathbf{a}_r}$, the lemma follows because the trace distance is an upper bound on the variation distance of the probability distribution resulting from making any measurement on these two states. □

6 Conclusions and Open Questions

We have established that it is NP-hard to approximate the value of both two-prover quantum entangled games and three-prover classical entangled games. These results leave open the case of *two*-prover one-round *classical* entangled games. Can our techniques be extended to this case?

The other obvious question is whether we can improve the inapproximability ratio to better than an inverse polynomial in the number of questions. Are there additional tests that further limit the advantage

provers can obtain by sharing entanglement? For example, in the case of classical entangled games, does it help to add more than three provers? In particular, if there are as many provers as there are questions, then sharing entanglement does not help, even if the verifier only talks to two provers chosen at random.

In very recent work [KKMV07] a subset of the authors obtain parallelization results for the case of quantum multi-round entangled games, showing that any such game with k provers and r rounds can be parallelized to a 3-turn game with k provers at the expense of a $\mathrm{poly}(r)$ factor in the value of the game. Moreover, such a game can be parallelized to 2 messages, or 1 round, by adding a $(k+1)$-st prover. We do not know whether it is possible to parallelize quantum entangled games from three to two messages without adding an additional prover.

There are a number of other important questions that our work does not address. Can we prove *upper* bounds on the hardness of computing the value of entangled games? It is instructive here to compare to the case where the provers share no-signalling correlations, where there is an efficient linear-programming algorithm to compute the value of a game [Pre].[22] In the quantum case, it is still not known whether the decision problem corresponding to finding the value of an entangled-prover game is recursive! The issue is that we are not currently able to prove any bounds on the amount of entanglement required to play a game optimally, even approximately.

7 Acknowledgments

We thank Tsuyoshi Ito, Jaikumar Radhakrishnan, Oded Regev, Amnon Ta-Shma, Mario Szegedy and Andy Yao for helpful discussions and John Watrous for pointing out that the optimal quantum value of a game might not be achieved with finite dimensional entanglement.

References

[Aar05] S. Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 1(1):1–28, 2005.

[Aar06] S. Aaronson. QMA/qpoly is contained in PSPACE/poly: De-Merlinizing quantum protocols. In *21st Annual IEEE Conference on Computational Complexity (CCC)*. 2006.

[ALM+98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[ANTV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM*, 49(4):496–511, 2002.

[Ara02] P. K. Aravind. The magic squares and Bell's theorem. Technical report, lanl-arXive quant-ph/0206070, 2002.

[AS98] S. Arora and S. Safra. Probabilistic checking of proofs; a new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16), September 26, 2001.

[Bel64] J. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[22] The reason that our proof does not work for no-signalling provers is that there is no notion of a partial measurement of a no-signalling probability distribution, so the classical strategy we use in our proofs cannot be defined.

[CCL94] J.-Y. Cai, A. Condon, and R. J. Lipton. PSPACE is provable by two provers in one round. *Journal of Computer and Systems Sciences*, 48(1):183–193, 1994.

[CGJ07] R. Cleve, D. Gavinsky, and R. Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive private information retrieval systems. Technical Report quant-ph/0707.1729, lanl arXiv, 2007. 12 July 2007.

[CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *IEEE Conference on Computational Complexity (CCC)*, pages 236–249. 2004.

[CSUU07] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Strong parallel repetition theorem for quantum XOR proof systems. In *Proc. of IEEE Conf. on Computational Complexity (CCC)*. 2007. To appear.

[DS01] K. Davidson and S. Szarek. Local operator theory, random matrices and banach spaces. In J. L. W. B. Johnson, editor, *Handbook on the Geometry of Banach spaces*, volume 1, pages 317–366. Elsevier Science, 2001.

[EL89] R. Exel and T. A. Loring. Almost commuting unitary matrices. *Proc. American Mathematical Society*, 106(4):913–915, 1989.

[GS89] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. JAI Press, 1989.

[GW07] G. Gutoski and J. Watrous. Toward a general theory of quantum games. In *Proceedings of 39th ACM STOC*, pages 565–574. 2007.

[Hal76] P. Halmos. Some unknown problems of unknown depth about operators on hilbert space. *Proc. Roy. Soc. A*, 76:67–76, 1976.

[Hås01] J. Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, 2001.

[IKP$^+$07] 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, 2007. Talk to be given at QIP'08, December 2007, Delhi, India.

[Kit] A. Kitaev. A bound on the cheating probability of strong quantum coin-flipping. Unpublished.

[KKMV07] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs, 2007. Talk to be given at QIP'08, December 2007, Delhi, India.

[KM03] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. Syst. Sci.*, 66(3):429–450, 2003.

[KMY03] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur? In T. Ibaraki, N. Katoh, and H. Ono, editors, *ISAAC*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198. Springer, 2003. ISBN 3-540-20695-7.

[KRT07] J. Kempe, O. Regev, and B. Toner. The unique games conjecture with entangled provers is false. Technical Report quant-ph/0710.0655, lanl arXiv, 2007. 02 October 2007.

[KV06] J. Kempe and T. Vidick. On the power of entangled quantum provers. Technical report, lanl-arXive quant-ph/0612063, 2006.

[KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proc. 32nd ACM Symp. on Theory of Computing*, pages 608–617. 2000.

[Lin97] X. Lin. Almost commuting selfadjoint matrices and applications. *Fields Inst. Commun.*, 13:193–233, 1997.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NPA07] M. Navascues, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98(1):010401, 2007. doi:10.1103/PhysRevLett.98.010401.

[Pre] D. Preda. Personal communication.

[Sha92] A. Shamir. IP = PSPACE. *J. ACM*, 39(4):869–877, 1992.

[She92] A. Shen. IP = PSPACE: simplified proof. *J. ACM*, 39(4):878–880, 1992. ISSN 0004-5411.

[Ton06] B. F. Toner. Monogamy of nonlocal quantum correlations. Technical report, 2006. quant-ph/0601172.

[Tsi87] B. S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *J. Soviet Math.*, 36:557–570, 1987.

[Voi83] D. Voiculescu. Asymptotically commuting finite rank unitary operators without commuting approximants. *Acta Sci. Math.*, 45:429–431, 1983.

[Wer89] R. F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Lett. Math. Phys.*, 17:359–363, 1989.

[Win99] A. Winter. *Coding Theorems of Quantum Information Theory*. Ph.D. thesis, Universit at Bielefeld, 1999. quant-ph/9907077.

[Yao] A. Yao. Personal communication, Feb. 2007.