2008 49th Annual IEEE Symposium on Foundations of Computer Science

Entangled games are hard to approximate

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

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

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

Ben Toner‡
CWI, Amsterdam

Thomas Vidick§
EECS, UC Berkeley

Abstract

We establish the first hardness results for the problem of computing the value of one-round games played by a referee and a team of players 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 referee and two entangled players or (ii) classical referee and three entangled players. 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-player games to make them resistant to entangled players. 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-player games cannot be computed by semidefinite programs that are polynomial in the size of the referee's system, a method that has been successful for more restricted quantum games.*

1 Introduction

Multi-player games have played a tremendous role in theoretical computer science over the last two decades. In this setting, several players, who are not allowed to communicate with each other during the game, exchange messages with a referee according to a prescribed protocol and try to convince him to accept. The *value* of a game is the maximum probability with which the players can achieve this, averaged over all the referee's questions and possibly over the shared randomness of the players. 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 referee. 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 [2, 3], which shows that the value of a two-player 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-player games in the quantum world, the laws of quantum mechanics allow for a fascinating new effect: namely, the players can share an arbitrary *entangled* state, on which they may perform any local measurements they like to help them answer the referee's questions. Such a game will be called an *entangled game*. The fact that entanglement can cause non-classical correlations is a familiar idea in quantum physics, introduced in a seminal 1964 paper by Bell [4]. Most importantly, there is no physical way to prevent players from sharing entanglement or to limit how much they have. Compare this to the restriction that the players cannot communicate during the game, which can be enforced physically by separating the players in space so that there is no time for a message to travel from

*Work partly done while at LRI, Univ. de Paris-Sud, Orsay. 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, by a grant of the Israeli Science Foundation and by a European Research Council (ERC) Starting Grant.

†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.

0272-5428/08 $25.00 © 2008 IEEE
DOI 10.1109/FOCS.2008.8

one to the other. It is thus a natural and important question to ask how shared entanglement between the players influences the value of the game, as entanglement can allow for new strategies. 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-player game. One of the most important questions in this field, which we answer in this paper, has been to determine whether computing the value of entangled games is at least NP-hard.

Two recent results give evidence that entangled games might actually be computationally much *easier* than their classical counterparts. First, Cleve et al. [8] showed that in the case of a particular class of two-player one-round games, XOR-games, the value when players are entangled can be computed (to exponential precision) in polynomial time. In contrast, Håstad [14] 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 players 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 to within 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 players. This is possible using an inner-product preserving embedding of vectors into two-outcome observables due to Tsirelson [33], 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-player games are easy, Kempe, Regev and Toner [18] 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-player 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 values of more general entangled games. More generally the semidefinite programming approach has often been successful when quantum communication is involved: for example Kitaev and Watrous [21] have shown that SDPs can exactly compute the value of *single*-player quantum games, Gutoski and Watrous proved that the value of quantum refereed games is as easy to compute as the value of classical refereed games, again via semidefinite programming [12], and Kitaev showed that the cheating probability for quantum coin-flipping protocols [20] can be computed by SDPs. Moreover, Navascues et al. [26] recently gave a hierarchy of SDP relaxations to approximate the value of an entangled two-player 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-player 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 games in the quantum world. We need to distinguish between two types of games: on one hand one can still restrict the (possiby entangled) players to classical communication; we call such games *classical entangled games*. On the other hand one can also allow the players to communicate *quantum* messages with a *quantum referee*; we call these games *quantum entangled games*. In both cases the hardness of computing the value of the game with entangled players was previously not known,[2] and we show NP-hardness in two cases: for two-player one-round *quantum entangled games* (in the first part of the paper) and for three-player 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 player one-round quantum entangled game G or

2. three player 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

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

[2] Kobayashi and Matsumoto [22] showed that when the communication and the referee are quantum, but the players 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.

on entangled games, the following immediate corollary is of interest:

Corollary 2. *The success probability of classical entangled* 3*-player or quantum entangled* 2*-player games cannot be computed by SDPs of polynomial size, unless* P = NP.

The results above leave open the case of *two*-player one-round *classical* entangled games. Our third result deals with this case, but has a 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 referee 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*-player *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 the IP = PSPACE result [25, 29] even with public-coin protocols [11, 30], our result implies PSPACE$\subseteq$ MIP$^*(2,1)_{1,1-\mathrm{poly}^{-1}}$. Again, no such result was previously known for these games. Due to lack of space we do not give the details of this result here. They can be found in [16].

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 [2, 3])**.** *There is a constant* $s < 1$ *such that it is* NP*-hard to decide, given a two-player 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-player one-round game and modify it to a two-player one-round quantum entangled game (or a three-player classical entangled game) 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 players 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 players. To this end—and this is a crucial difference from 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-player one-round game, significantly limits the use of entanglement by the players beyond its utility 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 [1]: 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 players 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 players do not entangle the message register with the entangled state they share. This allows us to get conditions that involve the players' operators (describing their strategies) on two *different* questions. The Swap-Test crucially requires that the messages are quantum.

In order to analyze classical entangled games 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 players 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 players can cheat in the Odd Cycle game of Ref. [8], but if we add a third player, then entangled players can perform no better than classical ones [32]. Moreover, after the completion of this work we have learned from A. Yao [36] about a way to add a third player to the Magic Square game such that as a result the winning probability of entangled players is ≈ 0.94. See "Related work" below for further discussion of a recent extension of this result.

For our third result on two-player classical entangled games, our reduction has the same spirit and similar analysis as in the previous two cases: here we start with a *single*-player multi-round game and modify it to a one-round game by introducing a second player to prevent the first player from entangling the answers of subsequent rounds. Our modification here mimics a construction of [6] used to prove that PSPACE has (non-entangled) two-player one-round proof 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 referee pairwise "almost commute" in some sense or "almost do not disturb" the entangled state. This means that the players' actions are "almost classical", in the sense that they allow us to take any strategy for the entangled game and convert it back to a strategy for 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 players, when receiving a question from the referee, 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 players 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 players 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 players 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 become more complicated in the case where the value of the entangled game is $1 - \varepsilon$. Now, the players' measurements 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 players 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 referee, 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 is similarly distributed to the scenario in the entangled game, where the player 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 lose an ε in precision. As a result, the success probability of this new unentangled strategy is also 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 players. 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 [13].[7] It was shown subsequently [34],[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, before finally being proved in [24] by a "long tortuous argument" [9] using von Neumann algebras, almost 20 years after the conjecture had been pub-

[5] In fact, we show that the construction in [6] still remains sound even with entangled players, albeit with a weaker soundness than in the classical case.

[6] Obviously, the players 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 [10].

licised. 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* (a projector is a Hermitian matrix P such that $P^2 = P$), where the norm is the Frobenius norm $\|A\|_F^2 = \mathrm{Tr}(A^\dagger A)$ (see Sec. 3.1):

Conjecture. *Let $W_1, \ldots, W_n$ be d-dimensional projectors such that for some $\varepsilon \geq 0$ and for all $i, j \in \{1, \ldots, n\}$ $\frac{1}{d}\|W_i W_j - W_j W_i\|_F^2 \leq \varepsilon$. Then there exists a $\delta \geq 0$, and pairwise commuting projectors $\tilde{W}_1, \ldots \tilde{W}_n$ such that $\frac{1}{d}\|W_i - \tilde{W}_i\|_F^2 \leq \delta$ 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., the best possible result. Moreover, when scaled up to the setting of interactive proofs, the conjecture with a constant δ implies inclusion of NEXP in $\mathrm{QMIP}^*(2, 1)$ and $\mathrm{MIP}^*(3, 1)$ with completeness 1 and soundness bounded away from 1.

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 hardness of approximation of the value of entangled two-player *quantum* games, posted to the arXiv earlier [19]; the present paper includes and supersedes these results. Since this paper had been made public, our techniques have already been applied by [15] to show similar results for *binary* three-player one-round classical entangled games. Ref. [15] also give a new upper-bound for the value of these games; or, as often called in this context, they give a new tripartite Tsirelson-inequality. After the completion of this work Cleve, Gavinsky and Jain [7] use a connection to private information retrieval schemes to show that succinctly given binary entangled classical games cannot be approximated in polynomial time. Their result does not apply 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-player games. To flesh 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 three-player classical entangled games. We discuss our results and open questions in Section 5.

2 Preliminaries

We assume basic knowledge of quantum computation [27].

Games. In this paper we study multi-player games, or cooperative games with imperfect information (henceforth *games*). We will only deal with one-round games played by N cooperative players against a referee. 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 $\bar{Q} = \{q_{i_1 \ldots i_N}\}_{(i_1,\ldots,i_N)\in[Q]^N}$ of questions and $\bar{A} = \{a_{i_1 \ldots i_N}\}_{(i_1,\ldots,i_N)\in[A]^N}$ 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]

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

where the W_i are the player'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 players.

The game G is played as follows: The referee 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 player k for $1 \leq k \leq N$ and receives the answer $a_{j_1 \cdots j_N} \in \bar{A}$ from the players. The players win the game if $V(a_{j_1 \cdots j_N} | i_1, \ldots, i_N) = 1$; otherwise the referee wins. The *value* of a game is the maximum winning probability of the players. The players 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 referee, the players, and the question and answer sets. A game G will be called

- *classical* if the referee, the player, 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 referee simply sends q_k to the k-th player 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 referee, and the question and answer sets are classical, but the players are quantum, and are allowed to share an a priori entangled

[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 players.

state $|\Psi\rangle$ of arbitrary dimension. This increases the set of possible strategies to quantum operations performed on the player's share of the entangled state. Note that no restrictions on $|\Psi\rangle$ (such as $|\Psi\rangle$ consisting of EPR pairs, or $|\Psi\rangle$ having bounded dimension) are currently known to hold without loss of generality. By standard purification techniques (see, e.g., [8]) one can assume that each player 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-player 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 referee and the players 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 on N subsystems and the referee sends its k-th part to the k-th player for $1 \le k \le N$ using a quantum channel. After receiving as answer an N-register quantum state $a_{j_1\cdots j_N} \in \bar{A}$, where the k-th player sends the k-th register, the referee 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 player 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 referee. The value of an entangled-player quantum game, ω_q^*, is given by Eq. (1) where $U = U_1\otimes\cdots\otimes U_N$ and

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

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] 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 games where the distribution π is symmetric under interchange of the players, and so is the referee. Such games have a symmetric optimal strategy. It is easy to show that this restriction holds without loss of generality, by first symmetrizing the referee (incurring at most a doubling of the number of questions), and then showing that the strategies of the players can be made symmetric with the same success probability (see [16]).

[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 $i_1,\ldots,i_N$.

3 Hardness of two-player entangled quantum games

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

Theorem 4. *There is a constant $s_q > 0$ such that it is* NP*-hard to decide, given a two-player 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 5. *It is* NP*-hard to decide, given a two-player quantum entangled game, whether its value is* 1.

We first describe how to modify a two-player classical game $G_c(2,\pi,V)$ with questions Q and answers A to a two-player *quantum* game of equal or higher value. As noted above, without loss of generality we can assume that the distribution $\pi(q,q')$ is symmetric, and that each question has a non-zero probability of being asked.

The modified quantum game. In the constructed quantum game G_q the referee sends quantum registers $|q,0\rangle_A$ and $|q',0\rangle_B$ to players 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 players 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 referee performs one of two tests, with equal probability:

Classical Test: The referee samples (q,q') according to the distribution $\pi(q,q')$, and sends $|q,0\rangle$ to player A and $|q',0\rangle$ to player B. Upon receiving these registers from the players, 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 classical game G_c.

Quantum Test: The referee 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

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

He keeps the first qubit and sends question and answer registers to players A and B. Upon receiving these registers from the players, 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 players, controlled on the question, simply write the answer that the classical unentangled players 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 players 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 [5] 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 players' private spaces on which the referee is unable to perform the swapping. This partial swap has been used in [21] to show parallelization for QIP, and in [23] to prove the inclusion QMA(3) $\subseteq$QMA(2) (conditioned on QMA(2) amplification being possible), 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 players, 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.

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

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 6. *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 6: Consider an optimal 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 referee. We first show that the strategy of the players is indeed essentially a classical entangled strategy.

Claim 7. *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 player's half of $|\Psi\rangle$ with $\sum_{a \in A} W_q^a = \mathrm{Id}$, such that each player's transformation can be 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 referee 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 players share some entangled state $|\Psi'\rangle$ (which includes their private workspace). A and B apply the same unitary transformation U (recall that we assumed without loss of generality that the strategies in the quantum game were symmetric). Since the players pass with probability 1 the classical test, and in particular the check that the question registers are $|q\rangle$ resp. $|q'\rangle$, it means that they do not change the question registers. 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 $\tilde{W}_q^a = (\langle a| \otimes \mathrm{Id}) \cdot U_q \cdot (|0\rangle \otimes \mathrm{Id})$, 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

[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.

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. It implies that all projectors W_q^a commute with each other (see below in "Rounding").

Claim 8.

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

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

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

$$= \frac{1}{2} \sum_{a,a'} |a\rangle|a'\rangle \Big(|+\rangle (W_q^a \otimes W_{q'}^{a'} + W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle + |-\rangle (W_q^a \otimes W_{q'}^{a'} - W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle \Big)$$

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 players 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 8 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 when acting on the same system*. 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 players 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 defer the details to a full version (in any case Theorem 5 follows from Theorem 4). □

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. We modify the game in exactly the same way as before; in order to prove Theorem 4 it suffices to prove, for s from the PCP Theorem:

Lemma 9. *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 $1 - \varepsilon$. The proof of this lemma is omitted from this abstract. The first step consists in showing that the strategies of the players are essentially projective measurements, as in Claim 7. We can then extract "almost commuting" conditions on the operators of the players, which allow us to give a good strategy (described in the introduction) for the original game. The interested reader will find more details in [16].

4 Hardness of three-player entangled classical games

In this section we give the main ideas of the proof of Theorem 1 for three-player entangled classical games, which we now state as:

Theorem 10. *There is a constant $s_3 > 0$ such that it is* NP*-hard to decide, given an entangled three-player 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, we modify any two-player classical game $G(2, \pi, V)$ to a three-player classical entangled game G', as described in the introduction, which essentially has the same number of answers. We describe this modification, and give a rough idea of the proof of its correctness, leaving the details to the full version of this abstract [16].

The modified three-player game. In the constructed game G' the referee chooses one of the players uniformly at random. Rename the chosen player Alice and call the other players Bob and Cleve. The referee 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 referee performs both tests at the same time. The consistency test plays the role of the Swap-Test, limiting the advantage gained by sharing entanglement.

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 players reply according to an optimal classical strategy (which as before can be assumed to be symmetric) 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 10, we need to show the following.

Lemma 11. *If $\omega^*(G') > 1 - \varepsilon$ then $\omega(G) > s$.*

Consider a quantum strategy for G' that succeeds with probability $1 - \varepsilon$. Since the game G' is symmetric, we can assume that this strategy is symmetric. Suppose that the players 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 player measures their part of $|\Psi\rangle$. Following standard arguments (extending the private space of the players) 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

$$\begin{aligned} p_q(aa'|qq') &= \mathrm{Tr}\left(W_q^a \otimes W_{q'}^{a'} \rho^{\mathrm{AB}}\right) \\ &= \langle\Psi| W_q^a \otimes W_{q'}^{a'} \otimes \mathrm{Id} \, |\Psi\rangle. \end{aligned} \tag{3}$$

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

$$\begin{aligned} \pi_2(q) &= \sum_a \mathrm{Tr}\left(W_q^a \otimes W_q^a \rho^{\mathrm{AB}}\right) \\ &= \sum_a \langle\Psi| W_q^a \otimes W_q^a \otimes \mathrm{Id} \, |\Psi\rangle \end{aligned} \tag{4}$$

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

Eqs. (3) and (4) clarify the role of the third player, 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 referee chooses two of the players at random (say Alice and Bob) and only sends questions to them, not interacting with the third player at all.[15] Cleve's presence would not be important if the players were executing a classical strategy, but it can (and does) make a difference if their strategy requires entanglement. Indeed, if there were only two players, 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* [35]. It is the crucial property that enables us to prove that a classical strategy for the original game G, defined in a similar fashion as in the case of quantum games, is "close enough" to the player's strategy in G'. We give the details of the proof of Lemma 11 in [16].

[15] 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 10.

5 Conclusions and open questions

We have established that it is NP-hard to approximate the value of both two-player quantum entangled games and three-player classical entangled games. These results leave open the case of *two*-player 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 players can obtain by sharing entanglement? For example, in the case of classical entangled games, does it help to add more than three players? In particular, if there are as many players as there are questions, then sharing entanglement does not help, even if the referee only talks to two players chosen at random. [16]

In very recent work [17] a subset of the authors obtain parallelization results for the case of quantum multi-round entangled games, showing that any such game with k players and r rounds can be parallelized to a 3-turn game with k players at the expense of a $\mathrm{poly}(r)$ factor in the value of the game. Moreover, such a game can be parallelized to 2 turns, or 1 round, by adding a $(k+1)$-st player. We do not know whether it is possible to parallelize quantum entangled games from three to two messages without adding an additional player.

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 players share no-signalling correlations, where there is an efficient linear-programming algorithm to compute the value of a game [28].[17] In the entangled-player case, it is still not known whether the decision problem corresponding to finding the value of an entangled-player game is recursive! The issue is that we are not currently able to prove any bounds

[16] A proof of this fact follows from Theorem 2 of [31] (see also [35]).

[17] The reason that our proof does not work for no-signalling players 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.

on the amount of entanglement required to play a game optimally, even approximately.

6 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 achievable with finite dimensional entanglement.

References

[1] P. K. Aravind. The magic squares and Bell's theorem. Technical report, arXiv:quant-ph/0206070, 2002.

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

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

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

[5] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, 2001.

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

[7] R. Cleve, D. Gavinsky, and R. Jain. Entanglement-resistant two-prover interactive proof systems and nonadaptive private information retrieval systems. Technical report, arXiv:0707.1729, 2007.

[8] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proc. 19th IEEE CCC*, pages 236–249, 2004.

[9] 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.

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

[11] 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.

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

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

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

[15] T. Ito, H. Kobayashi, D. Preda, X. Sun, and A. C.-C. Yao. Generalized Tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems. In *Proc. 23rd IEEE CCC*, pages 187–198, 2008.

[16] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. Technical report, arXiv:0704.2903, 2007.

[17] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. In *Proc. 23rd IEEE CCC*, pages 211–222, 2008.

[18] J. Kempe, O. Regev, and B. Toner. The unique games conjecture with entangled provers is false. In *Proc. 49th IEEE FOCS*, 2008.

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

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

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

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

[23] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Proc. 14th ISAAC*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198, 2003.

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

[25] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992.

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

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

[28] D. Preda. Personal communication.

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

[30] A. Shen. IP = PSPACE: Simplified proof. *J. ACM*, 39(4):878–880, 1992.

[31] B. M. Terhal, A. C. Doherty, and D. Schwab. Symmetric extensions of quantum states and local hidden variable theories. *Phys. Rev. Lett.*, 90(15):157903, 2003.

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

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

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

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

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