2012 IEEE 53rd Annual Symposium on Foundations of Computer Science

A multi-prover interactive proof for NEXP sound against entangled provers

(Extended abstract — Full version available as arXiv:1207.0550)

Tsuyoshi Ito
NEC Laboratories America, Inc.
Princeton, NJ, USA
Email: tsuyoshi@nec-labs.com

Thomas Vidick
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology
Cambridge, MA, USA
Email: vidick@csail.mit.edu

***Abstract*—We prove a strong limitation on the ability of entangled provers to collude in a multiplayer game. Our main result is the first nontrivial lower bound on the class MIP* of languages having multi-prover interactive proofs with entangled provers; namely MIP* contains NEXP, the class of languages decidable in non-deterministic exponential time. While Babai, Fortnow, and Lund (Computational Complexity 1991) proved the celebrated equality MIP = NEXP in the absence of entanglement, ever since the introduction of the class MIP* it was open whether shared entanglement between the provers could weaken or strengthen the computational power of multi-prover interactive proofs. Our result shows that it does not weaken their computational power: MIP* contains MIP.**

At the heart of our result is a proof that Babai, Fortnow, and Lund's multilinearity test is sound even in the presence of entanglement between the provers, and our analysis of this test could be of independent interest. As a byproduct we show that the correlations produced by any entangled strategy which succeeds in the multilinearity test with high probability can always be closely approximated using shared randomness alone.

***Keywords*-quantum interactive proofs; multiple provers; entanglement**

I. Introduction

Multiprover interactive proof systems [6] are at the heart of much of the recent history of complexity theory, and the celebrated characterization MIP = NEXP [4] is one of the cornerstones on which the PCP theorem [3], [2] was built. While the key assumption on the multiple provers in an interactive proof system is that they are not allowed to communicate, traditionally this has been taken to mean that their only distributed resource was shared randomness. In a quantum universe, however, it is natural to relax this assumption and allow the provers to share *entanglement*. While still not allowing them to communicate, this increases their ability to collude against the verifier by exploiting the nonlocal correlations allowed by entanglement. The corresponding complexity class MIP* was introduced in [11], raising a fundamental question: *what is the computational complexity of entangled provers?*

Even before their modern re-formulation in the language of multiplayer games, starting with the work of Bell in the 1960s [5] the strength of the nonlocal correlations that could be obtained from performing local measurements on entangled particles has been intensely investigated through the use of *Bell inequalities* (upper bounds on the strength of classical correlations) and *Tsirelson inequalities* (upper bounds on the strength of quantum correlations). Games, or proof systems, generalize this setup by introducing an additional layer of *interaction*: in this new context, we think of the experimenter (the verifier) as interacting with the physical devices (the provers) through the specific choice of settings (questions) that he makes, and the outcomes (answers) that he observes. The arbitrary state and measurements that are actually made inside the devices are reflected in the provers' freedom in choosing their strategy. The fundamental observation that quantum mechanics violates certain Bell inequalities translates into the fact that there exists interactive proof systems in which entangled provers can have a strictly higher success probability than could any classical, non-entangled provers.

A dramatic demonstration of this possibility is given by the Magic Square game [26], [28], a simple one-round game for which the maximum success probability of classical provers is 8/9, but there exists a *perfect* winning strategy for entangled provers. Cleve, Høyer, Toner, and Watrous [11] were the first to draw

Tsuyoshi Ito is supported in part by ARO/NSA grant W911NF-09-1-0569. He was also supported by grants from NSERC, CIFAR, QuantumWorks, MITACS, CFI, and ORF received while he was a postdoctoral fellow at the Institute for Quantum Computing and David R. Cheriton School of Computer Science, University of Waterloo, Canada.

Thomas Vidick is supported by the National Science Foundation under Grant No. 0844626. Part of this work was done while he was a graduate student in the Computer Science department at UC Berkeley, as well as during visits to the Perimeter Institute in Waterloo, Canada and NEC Labs America.

0272-5428/12 $26.00 © 2012 IEEE
DOI 10.1109/FOCS.2012.11

complexity-theoretic consequences from such *non-local* properties of entanglement. They study the class $\oplus$MIP of languages having two-prover interactive proofs in which there is a single round of interaction, each of the provers is restricted to answering a single bit, and the verifier only bases his accept/reject decision on the parity of the two bits that he received. While it follows from work of Håstad [14] that this class equals NEXP (and is thus as powerful as the whole of MIP) for an appropriate setting of completeness and soundness parameters, Cleve et al. show that the corresponding entangled-prover class $\oplus$MIP* *collapses* to EXP for any choice of completeness and soundness parameters that are separated by an inverse polynomial gap.[1]

Despite intense efforts, for a long time little more was known, and prior to our work the best lower bound on MIP* resulted from the trivial observation that multiple entangled provers are at least as powerful as a single prover, hence IP = PSPACE $\subseteq$ MIP*, where the first equality is due to [25], [31].[2] The main difficulty in improving this trivial lower bound is the following: while the PCP theorem gives us a variety of two-prover interactive proof systems for NEXP-complete problems, there is no a priori reason (see e.g. the Magic Square game, which has a similar structure to that of basic proof systems for MAX-3-XOR, or the aforementioned collapse of $\oplus$MIP*) that they should remain sound in the presence of entanglement. The fact that entanglement, as a shared resource, is poorly understood is also reflected in the complete absence of reasonable *upper bounds* on the complexity class MIP*: while the inclusion MIP $\subseteq$ NEXP is straightforward, we do not know of any limits on the *dimension* of entanglement that may be useful to the provers in a given interactive proof system, and as a result their maximum success probability is not even known to be computable (see [30], [12], [27] for more on this aspect).

Since existing protocols may no longer be sound in the presence of entanglement between the provers, previous work has focused on finding ways to *modify* a given protocol in a way that would make it *entanglement resistant*; that is, honest provers (in the case of a YES-instance) can convince the verifier without shared entanglement while dishonest provers (in the case of a NO-instance) cannot convince the verifier with high probability even with shared entanglement. This was the route taken in [21], [17], [16], which introduced techniques to limit the provers' use of their entanglement. They proved non-trivial lower bounds on variants of the class MIP*, but with error bounds that are weaker than the standard definitions allow for. These relatively weak bounds came as a result of the "rounding" technique developed in these works: by adding additional constraints to the protocol, one ensures that optimal entangled strategies are in a sense close to classical, un-entangled strategies. This closeness, however, was shown using a rounding procedure that had a certain "local" flavor, inducing a large loss in the quality of the approximation.[3]

In addition, [16], based on [21], showed that PSPACE has two-prover *one-round* interactive proofs with entangled provers, with perfect completeness and exponentially small soundness error. Prior to our work, this was the best lower bound known on single-round multi-prover interactive proof systems with entanglement.

Additional related work: Given the apparent difficulty of proving good lower bounds on the power of multi-prover interactive proof systems with entangled provers, researchers have studied a variety of related models. Maybe the most natural extension of MIP* consists in giving the verifier more power by allowing him to run in quantum polynomial-time, and exchange quantum messages with the provers. The resulting class is called QMIP* (the Q stands for "quantum verifier", while the * stands for "entangled provers"), and it was formally introduced in [24], where it was shown that QMIP* contains MIP* (indeed, the verifier can always force classical communication by systematically measuring the provers' answers in the computational basis). Little more is known of QMIP*; in fact it is believed to equal MIP* [9]. Ben-Or et al. [7] introduced a model in which the verifier is quantum and the provers are allowed communication but no entanglement, and showed that the resulting class contains NEXP. Other works attempt to characterize the power of MIP* systems using *tensor norms* [29], [20]; so far however such norms have either led to computable, but very imprecise, approximations, or have remained (to the best of our knowledge) intractable.

II. Results

Let MIP$^*(k, m, c, s)$ be the class of languages that can be decided by an m-round interactive proof system with k (possibly entangled) provers and with completeness c and soundness error s.[4] Our main result is the

[1] This was later improved [33] to the inclusion of $\oplus$MIP* in the class of two-message single-prover interactive proofs QIP(2) $\subseteq$ PSPACE [19].

[2] It was recently shown that quantum messages are no more powerful than classical messages in *single-prover* interactive proof systems [18]: QIP = PSPACE. That result, however, has no direct relationship with our work: in our setting the messages remain classical; rather the "quantumness" manifests itself in the presence of *entanglement* between the provers, which is a notion that only arises when more than one prover is present.

[3] See the "almost-commuting implies nearly-commuting" conjecture in [21] for more on this aspect.

[4] We refer to Appendix A for a more complete definition of the class MIP*.

following.

Theorem 1. *All languages in* NEXP *have a four-prover poly-round interactive proof system with perfect completeness and exponentially small soundness error against entangled provers. That is, for every $q \in \text{poly}$, it holds that*

$$\text{NEXP} \subseteq \text{MIP}^*(4, \text{poly}, 1, 2^{-q}).$$

Theorem 1 resolves a long-standing open question [24], showing that entanglement does not weaken the power of multi-prover interactive proof systems: together with the inclusion MIP $\subseteq$ NEXP, it implies that MIP $\subseteq$ MIP*. We note that the proof system in Theorem 1 does not require honest provers to use any entanglement in order to achieve perfect completeness in the case of a YES-instance. In other words, if we denote by MIP$^{\text{er}}$ the class of languages having entanglement resistant multi-prover interactive proof systems with bounded error, our proof of Theorem 1 shows that NEXP $\subseteq$ MIP$^{\text{er}}$. Because MIP$^{\text{er}} \subseteq$ MIP by definition, this implies MIP$^{\text{er}} =$ NEXP.

The interactive proof system used in the proof of Theorem 1 uses four provers and a polynomial number of rounds of interaction. We do not know if the number of provers can be reduced; however if one is willing to increase it by one then the amount of interaction required can be reduced to a single round, i.e. one message from the verifier to each prover, and one message from each prover to the verifier. Indeed, our proof system has the additional property of being *non-adaptive*: the verifier can select his questions for all the rounds before interacting with any of the provers. It is shown in [15] that a non-adaptive entanglement-resistant protocol may be parallelized to a single round of interaction at the cost of adding an extra prover. Applying this result to Theorem 1 gives the following corollary.

Corollary 2. *All languages in* NEXP *have a five-prover one-round interactive proof system with perfect completeness and soundness error against entangled provers bounded away from* 1 *by an inverse polynomial, that is:*

$$\text{NEXP} \subseteq \text{MIP}^*(5, 1, 1, 1 - 1/\text{poly}).$$

Prior results on the complexity of multi-prover interactive proofs with entangled provers have often been stated using the languages of *games* [11], [21], [22]. The main difference, in terms of computational complexity, is in the way the input size is measured. In the case of games the input is an explicit description of the game, including a list of all possible questions and valid answers, while in the setting of proof systems the messages may be described implicitly: it is their *length* that is polynomial in the input size.

Because of this difference in scaling, our results do not immediately imply any NP-hardness result in the setting of multi-player games with entangled players. Nevertheless, by adapting the proof of Theorem 1 and using the PCP theorem one can show the following. There is a constant $\kappa > 1$ and a procedure that, given as input an arbitrary 3-SAT formula with n variables and $m = \text{poly}(n)$ clauses, runs in time $2^{O(\log^\kappa n)}$ and produces an explicit description of a four-player game of size $S = 2^{O(\log^\kappa n)}$ (i.e. the number of rounds of interaction and the total number of questions and answers that can be sent and received is at most S). The game has the property that, if the 3-SAT formula was satisfiable, then there is a perfect strategy for the players, which does not require any entanglement. If, however, the 3-SAT formula was not satisfiable, then there is no strategy for the players, even using entanglement, that succeeds with probability greater than $1/2$.

If one could show the above with constant $\kappa = 1$ then it would follow that finding a constant-factor approximation to the maximum success probability of four entangled players in a game with polynomially many rounds and questions is NP-hard; our result is limited to obtaining some possibly large $\kappa > 1$. The main point, however, is that the hardness of approximation is up to *constant* factors. This is in contrast to all previous results which were limited to hardness of approximation up to factors approaching 1 very quickly as the input size grew (even after arbitrary sequential or even parallel repetition).[5]

At the heart of the proof of Theorem 1 is a soundness analysis of Babai, Fortnow, and Lund's *multilinearity test* in the presence of entanglement between the provers: we show that it is in a sense "immune" to the strong non-local correlations that entangled provers may in general afford. We believe that this analysis should be of wider interest, and we explain the test and give an overview of its analysis in the presence of entanglement in Section IV. We first outline the overall structure of our proof system in Section III. It is very similar to the one introduced by Babai, Fortnow, and Lund [4] to prove NEXP $\subseteq$ MIP; our contribution consists in proving its soundness against entangled provers.

[5]Cleve, Gavinsky, and Jain [10] obtained a constant-factor hardness result for games with constant answer size, but in which the number of questions sent by the verifier is *exponential*.

III. A PROTOCOL FOR NEXP

Our interactive proof system, just as the one by Babai et al.,[6] verifies membership in a specific NEXP-complete language, *Oracle-3-satisfiability* (see Problems 1 and 2 in Appendix B for a definition). We give a four-prover, poly-round interactive protocol for it that has perfect completeness and soundness error bounded away from 1 by an inverse-polynomial in the input size. (Theorem 1 is obtained by sequentially repeating this interactive proof system.)

Simplifying a little bit, the verifier in our protocol is given as input two integers n, N in unary (think of N as much larger than n, but still polynomial), a description of a finite field $\mathbb{F}$ of size N, and a low-degree polynomial $f : (\mathbb{F}^n)^3 \times (\mathbb{F})^3 \to \mathbb{F}$. His goal is to verify whether there exists a multilinear function $g : \mathbb{F}^n \to \mathbb{F}$ such that $f(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, g(\boldsymbol{x}), g(\boldsymbol{y}), g(\boldsymbol{z})) = 0$ for all $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \{0,1\}^n \subset \mathbb{F}^n$. If this is the case then the input is a YES-instance, whereas if for all functions g that are "close" to multilinear functions at least one of the constraints $f(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, g(\boldsymbol{x}), g(\boldsymbol{y}), g(\boldsymbol{z})) = 0$ is not satisfied then it is a NO-instance. The difficulty, of course, is that there are exponentially many constraints to verify, and *all* must be satisfied for the instance to be a YES-instance.

The protocol is divided into two distinct parts, which only weakly interact with each other. In the first part of the protocol, the verifier performs a polynomial-round *low-degree sum-check test* with a single prover, say the last prover. This test is based on ideas already introduced by Lund, Fortnow, Karloff, and Nisan [25] and can be used to verify that a low-degree function defined over $\mathbb{F}^k$ vanishes on all of $\{0,1\}^k$. We will apply it to the low-degree function $h : (\mathbb{F}^n)^3 \to \mathbb{F}$ defined by $h(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = f(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, g(\boldsymbol{x}), g(\boldsymbol{y}), g(\boldsymbol{z}))$. An important point for us is that, in the LFKN protocol, the verifier eventually only needs to evaluate h at a *single* point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in (\mathbb{F}^n)^3$ chosen uniformly at random.

Of course, the verifier only knows f, not g, and the goal of the second part of the protocol is for the verifier to learn the three values $g(\boldsymbol{x}), g(\boldsymbol{y}), g(\boldsymbol{z})$. Note that here the function g is arbitrary (we are trying to verify its existence), *except that it has to be multilinear*. Hence the verifier will perform one of two tests with the three remaining provers: either directly ask them for the values $g(\boldsymbol{x}), g(\boldsymbol{y}), g(\boldsymbol{z})$, or perform a certain "multilinearity test", which enforces that, however the provers answer their queries, it must be according to a function that is close to a multilinear function. The two tests will be indistinguishable from the point of view of the provers because the marginal distribution on the question to each prover is uniform over $\mathbb{F}^n$ in both cases.

Completeness of the protocol is easy to verify, and in the case of a YES-instance honest provers do not need any entanglement to be accepted with probability 1. To prove soundness, assuming four entangled provers succeed with probability that is polynomially close to 1, we wish to conclude that the instance given as input to the verifier must be a YES-instance.

Note that provers successful in the overall protocol must, in particular, succeed with high probability in the multilinearity test. The key step in the analysis consists in showing the following: Any three entangled provers that succeed in the multilinearity test with high probability are "indistinguishable" from *classical* provers who use shared randomness to jointly sample a multilinear function g, and then answer question $\boldsymbol{x}$ with $g(\boldsymbol{x})$. This step is the one that requires the most work, and we explain it in more detail in the next section. (In particular, we will clarify what is meant by "indistinguishable".)

Assuming this informal statement holds, it is not too hard to conclude the analysis of the protocol. Indeed, having replaced the three provers used in the multilinearity test by three classical provers, there is only a single "quantum" prover left, the one used to perform the sum-check test in the first part of the protocol. But entanglement cannot be useful to a single prover, and hence we may also assume that this last prover behaves classically. Since all provers are now classical, we have reduced our analysis to the classical setting and can appeal to the results in [4] to conclude. We refer to the full version for a more detailed presentation and soundness analysis of the protocol.

IV. THE MULTILINEARITY GAME

The key step in the proof of Theorem 1 is the analysis of the multilinearity test of [4], which generalizes the celebrated *linearity test* of Blum, Luby, and Rubinfeld [8] and is essential in constructing a protocol for NEXP that has messages of polynomial length.[7] The test can be formulated as a game played between the verifier and three players. The game is parametrized by a finite field $\mathbb{F}$ and an integer n. In the game, the verifier performs either of the following with probability 1/2 each:

[6] We emphasize that the proof system we use is not new, as it is essentially the same as the one introduced in [4]. We nevertheless outline it because there is a small difference in how the "oracle" in [4] is simulated by provers, which is the reason our protocol, unlike the one in [4], requires more than two provers.

[7] One can devise a protocol based on the linearity test alone, but it requires the verifier to send messages with exponential length to the provers. Such use of the linearity test was already key in establishing the early result NP = PCP(poly, 1); see e.g. Theorem 2.1.10 in [2].

- *Consistency test.* The verifier chooses $\boldsymbol{x} \in \mathbb{F}^n$ uniformly at random and sends the same question $\boldsymbol{x}$ to all three players. He expects each of them to answer with an element of $\mathbb{F}$, and accepts if and only if all the answers are equal.
- *Linearity test.* The verifier chooses $i \in \{1, \ldots, n\}$, $\boldsymbol{x} \in \mathbb{F}^n$ and $y_i, z_i \in \mathbb{F}$ uniformly at random, and sets $y_j = z_j = x_j$ for every $j \in \{1, \ldots, n\} \setminus \{i\}$. He sends $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ to the three players, receives $a, b, c \in \mathbb{F}$, and accepts if and only if

$$\frac{b-a}{y_i - x_i} = \frac{c-b}{z_i - y_i} = \frac{c-a}{z_i - x_i}.$$

Babai, Fortnow, and Lund show that, if any three *deterministic* players are accepted by the verifier with probability at least $1 - \varepsilon$ in this game, then the functions they each apply to their questions in order to determine their respective answers are close to a single *multilinear* function $g : \mathbb{F}^n \to \mathbb{F}$ (see Theorem 4.16 in [4] for an analysis of a variant of the test over the integers). That is, for all but at most a fraction roughly $O(n^2\varepsilon)$ (provided $|\mathbb{F}|$ is large enough) of $\boldsymbol{x} \in \mathbb{F}^n$, the players' answer to question $\boldsymbol{x}$ is precisely $g(\boldsymbol{x})$.

A major hurdle in proving a similar statement in case the players are allowed to use quantum mechanics already arises in *formulating* the statement to be proven: even in the case of players restricting their use of entanglement as shared randomness, what meaning should one ascribe to their strategies being "close to multilinear"? Indeed, it could be that the answer of each player to a fixed question, when taken in isolation, is uniformly random: the whole substance of the strategy is in the *correlations* between the answers of different players. This difficulty is usually set aside by "fixing the randomness". Entanglement, however, cannot be "fixed", and this forces us to face even the presumably simpler case of randomized strategies head on. We show that the following is an appropriate formulation of Babai et al.'s multilinearity test in the general setting of entangled (or even just randomized) players.

Theorem 3 (Informal)**.** *Suppose that three entangled players who share a permutation-invariant state $|\Psi\rangle$ succeed in the multilinearity game with probability $1 - \varepsilon$ where each player uses the set of measurements*[8] *$\{A^a_{\boldsymbol{x}}\}_{a \in \mathbb{F}}$ to determine his answer to the verifier's question $\boldsymbol{x} \in \mathbb{F}^n$.*

Then there exists a single *measurement $\{V^g\}$, independent of any question and with outcomes in the set of all multilinear functions $g : \mathbb{F}^n \to \mathbb{F}$, such that, in the multilinearity game, each player's action is* indistinguishable *from that of player whom, upon receiving his question $\boldsymbol{x}$, would*

1) *Measure his share of $|\Psi\rangle$ with $\{V^g\}$, obtaining a multilinear function g as an outcome,*
2) *Answer his question $\boldsymbol{x}$ with $g(\boldsymbol{x})$.*

Moreover, the multilinear functions used by the three players are identical with high probability.

In case the players are classical, but may use shared randomness, the theorem makes the following simple statement: players successful in the multilinearity game are "indistinguishable" from players who would first look up their random string, based on that alone select a multilinear function g, and finally answer their respective questions $\boldsymbol{x}_i$ with $g(\boldsymbol{x}_i)$. While such a statement is a direct corollary of Babai, Fortnow, and Lund's analysis, our contribution is to prove it without first "fixing the randomness" — and to show that it also holds for the case of players using entanglement.

An appropriate notion of distance on entangled-prover strategies: Crucial to the applicability of Theorem 3 is the precise notion of "indistinguishability" used. Indeed, while there is no hope of making statements on the players' measurements or their shared entangled state themselves (since the verifier has no direct access to them throughout the protocol), one still needs to use a notion that is strong enough to be meaningful even when the multilinearity game is executed as a building block in the larger protocol explained in the previous section.

The measure we use is based on the notion of *consistency* between two measurements, and we introduce it here in a simplified setting (we refer to the full version for more complete definitions). Let $\{A^i\}_{i \in I}$ and $\{B^i\}_{i \in I}$ be two quantum measurements of the same dimension and indexed by the same set of outcomes: $A^i, B^i \geq 0$ for all $i \in I$, and $\sum_i A^i = \sum_i B^i = \mathrm{Id}$. Let $|\Psi\rangle$ be a bipartite state that is invariant under permutation of its two subsystems, and ρ its reduced state on either. We say that A and B are *ε-consistent* if the following holds:

$$\mathrm{CON}(A, B) := \sum_i \langle \Psi | A^i \otimes B^i | \Psi \rangle \geq 1 - \varepsilon. \qquad (1)$$

This definition has an operational interpretation: the two measurements A and B, when performed on the two subsystems of $|\Psi\rangle$, give the same outcome except with probability ε . The key fact about consistent measurements is the following. Suppose that A and A, B and B, and A and B are all ε-consistent. Then A and B are *indistinguishable* in the sense that

$$\sum_i \left\| \sqrt{A^i} \rho \sqrt{A^i} - \sqrt{B^i} \rho \sqrt{B^i} \right\|_1 = O(\sqrt{\varepsilon}). \qquad (2)$$

[8] A measurement is a collection of non-negative matrices $\{P^a\}_{a \in A}$ such that $\sum_a P^a = \mathrm{Id}$ (this is usually called a *Positive Operator-Valued Measure*, or POVM).

This last expression corresponds to a more familiar notion of closeness of two measurements: they are close if the post-measurement states resulting from applying either are close in trace distance. The fact that (1) essentially implies (2) relies on Winter's "gentle measurement" lemma [34, Lemma 9] (see also Aaronson's "almost as good as new" lemma [1, Lemma 2.2]), a key tool in our analysis.

Henceforth we will consider two measurements to be close whenever they are consistent, having the assurance that this notion of closeness implies the more traditional one expressed by (2). In particular, it is not hard to verify that (2) implies that either measurement may be "replaced" by the other even in a wider context; for lack of space we refer to the full version for more details on how this can be done. The advantage of using the notion of ε-consistency is that it arises naturally from the analysis of the multilinearity game, and it is a notion that is very convenient to work with.

Rounding entangled strategies in the multilinearity game: Theorem 3 states that success in the multilinearity game forces even entangled players to make a trivial use of their entanglement: since the measurement $\{V^g\}$ is independent of their respective questions, they might as well perform it before the game starts, in which case they are not using their entanglement at all. Hence the theorem implies that entangled players are no more powerful than classical players in that game. A key insight of our work, however, is to avoid any attempt to prove such a statement *directly*. Instead, our proof technique consists in progressively manipulating the players' strategies themselves, without *explicitly* trying to relate them to a classical strategy.

Our goal is to show how the measurement $\{V^g\}$ can be extracted from the initial set of measurements $\{A^a_{\boldsymbol{x}}\}$ which depend on $\boldsymbol{x} \in \mathbb{F}^n$.[9] More precisely, we show how, starting from the original measurements $\{A^a_{\boldsymbol{x}}\}$, one may remove the dependence of $\{A^a_{\boldsymbol{x}}\}$ on $\boldsymbol{x} \in \mathbb{F}^n$ one coordinate at a time — eventually reaching the measurement $\{V^g\}$. Towards this we construct a sequence of measurements $\{B^g_{x_{k+1},\ldots,x_n}\}_g$, for $k = 1, \ldots, n$, with outcomes g in the set of multilinear functions $\mathbb{F}^k \to \mathbb{F}$. Each of these measurements has the following key property: the respective strategies corresponding to (i) measuring according to $\{A^a_{\boldsymbol{x}}\}$ and answering a or (ii) measuring according to $\{B^g_{x_{k+1},\ldots,x_n}\}$ and answering $g(x_1, \ldots, x_k)$ are *consistent*, in the sense described in Eq. (1): two distinct players using either strategy will obtain the same answer with high probability (provided they started with the same question).

This sequence of measurements is defined by induction, and we only explain the one-dimensional case here. Our construction is intuitive: $\{B^g\}$ corresponds to measuring using $\{A^a_{x_1}\}$ twice, *in succession*, using two randomly chosen values of x_1, and returning the unique linear function g which interpolates between the two outcomes obtained. This can be interpreted as a quantum analogue of the reconstruction procedure already used in the linearity test of Blum, Luby, and Rubinfeld: to recover a linear function it suffices to evaluate it at two random points, and then interpolate. We refer the reader to the full version for the general claim, which states a quantum analogue of Babai et al.'s "pasting lemma" [4, Lemma 5.11].

An additional hurdle arises as a result of the induction: the quality of the approximation between the original measurements $\{A^a_{\boldsymbol{x}}\}$ and the constructed measurements $\{B^g_{x_{k+1},\ldots,x_n}\}$ blows up *exponentially* with k. In order to control this error, one has to perform an additional step of *self-improvement*. This step was a key innovation in the work of Babai, Fortnow, and Lund, and extending it to the setting of entangled strategies requires substantially more work. While for the case of deterministic strategies Babai et al. were able to show, using the expansion properties of the hypercube, that any "reasonably good" k-linear approximation g at any point in the induction was automatically "extremely good", in our case we need to actively update the measurements through a self-correction procedure, obtaining the "improved" measurements as the optimum of a certain convex optimization problem. The need for such active correction is not a limitation of our approach, but rather reflects a fundamental difference between the quantum and the classical, deterministic settings: while two binary-valued functions either fully agree or fully disagree at any point, two quantum measurements can produce outcomes according to distinct but arbitrarily close distributions (think of one of the measurements as being obtained from the other by a small perturbation, such as an arbitrarily small rotation). It is this kind of "error" that needs to be corrected, and we refer to the full version for more detailed explanations on how this is done.

V. Discussion and open questions

Improving the parameters in Theorem 1 and Corollary 2 is an open problem. For example, it might be possible to reduce the number of provers to two, and the number of rounds of interaction to one, while still preserving exponentially small soundness error, resulting in the inclusion NEXP $\subseteq$ MIP$^*(2, 1, 1, 2^{-q})$ for every polynomial q. This would be an analogue of the known containment NEXP $\subseteq$ MIP$(2, 1, 1, 2^{-q})$ [13].

[9] While we do give an explicit, inductive algorithmic procedure showing how $\{V^g\}$ can be constructed, this is not necessary: the point is only in proving its *existence*.

Our overall protocol for NEXP requires four provers, and five provers if we would like to parallelize it by using [15]. We leave the problem of reducing the number of provers to fewer than four for future work. It may also be possible to improve the soundness guarantees in Corollary 2 by using the parallel repetition techniques from [23], but we have not explored this possibility.

In comparison to the PCP theorem, there are important parameters which are not explicit in Theorem 1 and Corollary 2: the amount of randomness used by the verifier and the total answer length. In our constructions, both of them are just bounded by a polynomial in the input length for NEXP, and they are poly-logarithmic for the scaled-down version corresponding to verification of languages in NP. If these numbers are respectively reduced to a logarithm and a constant for NP with a constant soundness, the result will be an analogue of the PCP theorem in presence of entanglement. Obtaining such a result may require extending our analysis of the multilinearity test to the more powerful *low-degree* tests that were key to establishing the "scaled-down" version of the PCP theorem.

Honest provers in our protocol do not need entanglement in order to achieve completeness 1 in the case of a YES-instance. It remains open whether entanglement can have any positive use in this context: is MIP* strictly larger than MIP = NEXP?

Acknowledgments

Tsuyoshi Ito thanks John Watrous for helpful discussions. Thomas Vidick thanks Umesh Vazirani for many inspiring discussions throughout the time that this work was being carried out, and in particular for first suggesting to adapt Babai et al.'s multilinearity test to the entangled-prover setting. The authors also thank Scott Aaronson, Dmitry Gavinsky, Oded Regev, and an anonymous referee for helpful suggestions.

References

[1] S. Aaronson, "Limitations of quantum advice and one-way communication," *Theory of Computing*, vol. 1, no. 1, pp. 1–28, 2005.

[2] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *Journal of the ACM*, vol. 45, no. 3, pp. 501–555, 1998.

[3] S. Arora and S. Safra, "Probabilistic checking of proofs: A new characterization of NP," *Journal of the ACM*, vol. 45, no. 1, pp. 70–122, 1998.

[4] L. Babai, L. Fortnow, and C. Lund, "Non-deterministic exponential time has two-prover interactive protocols," *Computational Complexity*, vol. 1, pp. 3–40, 1991.

[5] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics*, vol. 1, pp. 195–200, 1964.

[6] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson, "Multi-prover interactive proofs: How to remove intractability assumptions," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*, 1988, pp. 113–131.

[7] M. Ben-Or, A. Hassidim, and H. Pilpel, "Quantum multi prover interactive proofs with communicating provers," in *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, 2008, pp. 467–476.

[8] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," *Journal of Computer and System Sciences*, vol. 47, no. 3, pp. 549–595, 1993.

[9] A. Broadbent, J. Fitzsimons, and E. Kashefi, "QMIP = MIP*," arXiv:1004.1130, Tech. Rep., 2010.

[10] R. Cleve, D. Gavinsky, and R. Jain, "Entanglement-resistant two-prover interactive proof systems and non-adaptive PIR," *Quantum Information and Computation*, 2009.

[11] R. Cleve, P. Høyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies," in *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, 2004, pp. 236–249.

[12] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, "The quantum moment problem and bounds on entangled multi-prover games," in *Proceedings of the 23rd IEEE Annual Conference on Computational Complexity*, 2008, pp. 199–210.

[13] U. Feige and L. Lovász, "Two-prover one-round proof systems: Their power and their problems," in *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, 1992, pp. 733–744.

[14] J. Håstad, "Some optimal inapproximability results." *Journal of the ACM*, vol. 48, pp. 798–859, 2001.

[15] T. Ito, "Parallelization of entanglement-resistant multi-prover interactive proofs," 2011, submitted.

[16] T. Ito, H. Kobayashi, and K. Matsumoto, "Oracularization and two-prover one-round interactive proofs against nonlocal strategies," in *Proceedings of the 24th IEEE Annual Conference on Computational Complexity*, 2009, pp. 217–228.

[17] 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 *Proceedings of the 23rd IEEE Conference on Computational Complexity*, 2008, pp. 187–198.

[18] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous, "QIP = PSPACE," *Journal of the ACM*, vol. 58, no. 6, pp. 30:1–30:27, 2011.

[19] R. Jain, S. Upadhyay, and J. Watrous, "Two-message quantum interactive proofs are in PSPACE," in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, 2009, pp. 534–543.

[20] M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, and M. M. Wolf, "Operator space theory: A natural framework for bell inequalities," *Phys. Rev. Lett.*, vol. 104, p. 170405, Apr 2010.

[21] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick, "Entangled games are hard to approximate," *SIAM Journal on Computing*, vol. 40, no. 3, pp. 848–877, 2011.

[22] J. Kempe, O. Regev, and B. Toner, "Unique games with entangled provers are easy," *SIAM Journal on Computing*, vol. 39, no. 7, pp. 3207–3229, 2010.

[23] J. Kempe and T. Vidick, "Parallel repetition of entangled games," in *Proceedings of the 43rd Annual ACM Symposium on the Theory of Computing*, San Jose CA, 2011, pp. 353–362.

[24] H. Kobayashi and K. Matsumoto, "Quantum multi-prover interactive proof systems with limited prior entanglement," *Journal of Computer and System Sciences*, vol. 66, no. 3, pp. 429–450, 2003.

[25] C. Lund, L. Fortnow, H. Karloff, and N. Nisan, "Algebraic methods for interactive proof systems," *Journal of the ACM*, vol. 39, pp. 859–868, 1992.

[26] N. D. Mermin, "Simple unified form for the major no-hidden-variables theorems," *Phys. Rev. Lett.*, vol. 65, pp. 3373–3376, 1990.

[27] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New Journal of Physics*, vol. 10, no. 073013, 2008.

[28] A. Peres, "Incompatible results of quantum measurements," *Physics Letters A*, vol. 151, no. 3-4, pp. 107–108, 1990.

[29] A. Rapaport and A. Ta-Shma, "On the power of quantum, one round, two prover interactive proof systems," *Quantum Information Processing*, vol. 6, pp. 445–459, 2007.

[30] V. B. Scholz and R. F. Werner, "Tsirelson's Problem," arXiv:0812.4305, Tech. Rep., 2008.

[31] A. Shamir, "IP = PSPACE," *Journal of the ACM*, vol. 39, no. 4, pp. 869–877, 1992.

[32] B. S. Tsirelson, "Quantum generalizations of Bell's inequality," *Letters in Mathematical Physics*, vol. 4, no. 2, pp. 93–100, 1980.

[33] S. Wehner, "Entanglement in interactive proof systems with binary answers," in *Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science*, ser. Lecture Notes in Computer Science, vol. 3884, 2006, pp. 162–171.

[34] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2481–2485, 1999.

APPENDIX

A. Multi-prover interactive proofs

In this appendix we define the complexity classes that this work is concerned with: multi-prover interactive proof systems (MIP systems) and multi-prover interactive proof systems *with entanglement* (MIP* systems).

Let $k(n)$ be an integer, denoting the number of provers, and $m(n)$ an integer denoting the number of rounds. Both $k(n)$ and $m(n)$ are from the set of polynomially bounded, polynomial-time computable functions in the input size $|x|$, denoted by poly. Further, c and s denote polynomial-time computable functions of the input size into $[0,1]$ corresponding to completeness acceptance probability and soundness error. For notational convenience in what follows we will omit the arguments of these functions.

*Multi-prover interactive proof systems (*MIP *systems):* Let $k, m, l \in$ poly. A k-prover interactive proof system consists of a verifier V and k provers $P_1, \ldots, P_k$. The verifier is a probabilistic polynomial-time Turing machine, and the provers are computationally unbounded. Each of them has a read-only input tape and a private work tape. Each prover has a communication tape. The verifier has a random tape. The verifier also has k communication tapes, one for each prover, each of which is l bits long.

The input tape for every party contains the same input string x. The protocol consists of $m(|x|)$ rounds. In each round, first the verifier runs for a polynomial amount of time, updating the work and communication tapes. After that, the content of the ith communication tape is sent to the ith prover for each $i = 1, \ldots, k(|x|)$. Each prover reads this string, updates the content of his own work tape, and decides a reply to the verifier. The reply from the ith prover is written in the ith communication tape, and this round completes. After $m(|x|)$ rounds of interaction, the verifier produces a special output bit, designating acceptance or rejection. The operations by provers are instantaneous and do not have to be even computable; the provers are assumed to be able to "compute" any function.

For simplicity, we assume that each message between the verifier and the provers in each round is exactly l bits long for the purpose of a formal definition, but it is not hard to modify the definition to incorporate the more general case which does not satisfy this assumption. Formally, a *strategy* for $P_1, \ldots, P_k$ in a k-prover m-round interactive proof system consists

of the length $l' \in \mathbb{N}$ of a work tape, and km mappings $f_{ij}\colon \{0,1\}^l \times \{0,1\}^{l'} \to \{0,1\}^l \times \{0,1\}^{l'}$ for $1 \leq i \leq k$ and $1 \leq j \leq m$. Each mapping f_{ij} specifies the operation which prover i performs in round j: $f_{ij}(q,w) = (q',w')$ means that if the message from the verifier in this round is q and the work tape contains string w before the operation by the prover, then the message to the verifier in this round is q' and the work tape contains string w after the operation.

Definition 4. *Let $k,m\colon \mathbb{N} \to \mathbb{N}$, and let $c,s\colon \mathbb{N} \to [0,1]$ such that $c(n) > s(n)$ for all $n \in \mathbb{N}$. A language L is in $\mathrm{MIP}(k,m,c,s)$ if and only if there exists an m-round polynomial-time verifier V for a k-prover interactive proof system such that, for every input x:*

(Completeness) *if $x \in L$, there exists a strategy for provers $P_1,\dots,P_k$ such that the interaction protocol of V with $(P_1,\dots,P_k)$ results in the verifier accepting with probability at least c,*
(Soundness) *if $x \notin L$, for any strategy for provers $P'_1,\dots,P'_k$, the probability that the interaction protocol of V with $(P_1,\dots,P_k)$ results in the verifier accepting is at most s.*

In this formulation, the provers are deterministic, but this is not a limitation because it is well-known that the power of the model does not change if we allow the provers to share a random source.

If some of the parameters k, m, c, and s are sets of functions instead of single functions, the class is interpreted to be the union over all choices in the sets. For example,

$$\mathrm{MIP}(5,1,1,1-1/\operatorname{poly}) = \bigcup_{f\in\mathrm{poly}} \mathrm{MIP}(5,1,1,1-1/f).$$

We denote $\mathrm{MIP}(\mathrm{poly},\mathrm{poly},2/3,1/3)$ simply by MIP.

*Multi-prover interactive proof systems with entanglement (*MIP* *systems):* First introduced in [11], MIP* systems are defined analogously to MIP systems. The only difference is that now the provers are allowed to be *quantum*, while the verifier (and communication) remains bounded in classical probabilistic polynomial-time. This implies that the provers may share an arbitrary entangled state $|\Psi\rangle$ among themselves before the protocol starts and that each prover may use his part of the entangled state to determine his reply to the verifier. In each round, the provers individually receive the messages from the verifier in a message register, perform a quantum operation on this register together with their share of the entangled state, measure the message register in the computational basis, and send back the outcome to the verifier.

Formally, an *entangled strategy* for $P_1,\dots,P_k$ in a k-prover m-round interactive proof system with entanglement consists of the length $l' \in \mathbb{N}$ of a work tape, km quantum channels Φ_{ij} from a quantum register of $l+l'$ qubits to itself for $1 \leq i \leq k$ and $1 \leq j \leq m$, and the initial quantum state $|\Psi\rangle$ of the work tape, which is a kl'-qubit state. Each channel Φ_{ij} specifies the operation which prover i performs in round j: the first l qubits in the state correspond to the message from and to the verifier, and the last l' qubits represent the content of the work tape. After the prover's operation, the first l qubits are measured in the computational basis and sent to the verifier.

Definition 5. *A language L is in $\mathrm{MIP}^*(k,m,c,s)$ if and only if there exists an m-round polynomial-time verifier V for k-prover interactive proof systems such that, for every input x:*

(Completeness) *if $x \in L$, there exists an entangled strategy for provers $P_1,\dots,P_k$ such that the interaction protocol of V with $(P_1,\dots,P_k)$ results in the verifier accepting with probability at least c,*
(Soundness) *if $x \notin L$, for any entangled strategy for provers $P'_1,\dots,P'_k$, the probability that the interaction protocol of V with $(P_1,\dots,P_k)$ results in the verifier accepting is at most s.*

In certain cases, we can simplify part of the definition of entangled strategies. Suppose that the verifier interacts with certain prover P_i only once; i.e., the verifier is guaranteed to send P_i the empty string (or a fixed string) in rounds other than round j, and is guaranteed to ignore the reply from P_i in rounds other than round j. In this case, instead of specifying m quantum channels to describe the behavior of P_i in the m rounds, we may just specify measurements $A_q = (A_q^r)$ for each message q from the verifier, where the outcome of each measurement gives a reply to the verifier.[10] Since all the interactive proof systems considered in this paper have the property that the verifier interacts with each prover only once except for one prover, we use this simplified formulation in many places.

Note that we do not assume any upper bound on the size l' of the work tape used by each prover (in particular, we do not assume that $l' \in \mathrm{poly}$; the model with this restriction is considered in [24]). However, we do assume that they only use a finite-dimensional Hilbert space. A more general definition is commuting-operator provers, considered by Tsirelson [32] in the context of Bell inequalities and later in [30], [12], [27], [17]. Although we expect that our results remain valid with minor modifications to the proofs even if dishonest provers are allowed to use arbitrary commuting-operator strategies, we have not explored this possibility.

[10] Any classical post-processing by the prover can be incorporated as part of the description of his measurement.

B. NEXP-*complete problems*

Our results are based on the following NEXP-complete problem, as stated in Proposition 4.2 of Ref. [4]:

Problem 1: Oracle-3-satisfiability.
Instance. Integers $r, n \in \mathbb{N}$ in unary and a Boolean formula $B(\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, a_1, a_2, a_3)$ in variables $\boldsymbol{z} \in \{0,1\}^r$, $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3 \in \{0,1\}^n$ and $a_1, a_2, a_3 \in \{0,1\}$.

Question. Does there exist $A\colon \{0,1\}^n \to \{0,1\}$ such that $B(\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, A(\boldsymbol{b}_1), A(\boldsymbol{b}_2), A(\boldsymbol{b}_3)) = 1$ simultaneously for all $\boldsymbol{z} \in \{0,1\}^r$ and $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3 \in \{0,1\}^n$?

Using the standard technique of arithmetization (see e.g. Proposition 3.1 and Lemma 7.1 of Ref. [4]), one can show that the following problem is also NEXP-complete.

Problem 2: Oracle-3-satisfiability, arithmetized version.
Instance. Integers $r, n \in \mathbb{N}$ in unary and an arithmetic expressionfor a polynomial $f(\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, a_1, a_2, a_3)$, where $\boldsymbol{z}$ represents r variables and each of $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$ represents n variables.

Yes-promise. There exists an $A\colon \{0,1\}^n \to \{0,1\}$ such that for all $\boldsymbol{z} \in \{0,1\}^r$ and all $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3 \in \{0,1\}^n$, it holds that

$$f(\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, A(\boldsymbol{b}_1), A(\boldsymbol{b}_2), A(\boldsymbol{b}_3)) = 0 \qquad (3)$$

in $\mathbb{Z}$ (and therefore in every field).

No-promise. For every pair $(\mathbb{F}, A)$ of a field $\mathbb{F}$ and a mapping $A\colon \{0,1\}^n \to \mathbb{F}$, there exist $\boldsymbol{z} \in \{0,1\}^r$ and $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3 \in \{0,1\}^n$ such that Eq. (3) is not satisfied in $\mathbb{F}$.

We note that the degree of the polynomial f represented by the arithmetic expression can be at most the size of the arithmetic expression, and is therefore bounded by the input size.