Entanglement in Interactive Proof Systems with Binary Answers

Stephanie Wehner*

CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
wehner@cwi.nl

Abstract. If two classical provers share an entangled state, the resulting interactive proof system is significantly weakened [6]. We show that for the case where the verifier computes the XOR of two binary answers, the resulting proof system is in fact no more powerful than a system based on a single quantum prover: $\oplus\text{MIP}^*[2] \subseteq \text{QIP}(2)$. This also implies that $\oplus\text{MIP}^*[2] \subseteq \text{EXP}$ which was previously shown using a different method [7]. This contrasts with an interactive proof system where the two provers do not share entanglement. In that case, $\oplus\text{MIP}[2] = \text{NEXP}$ for certain soundness and completeness parameters [6].

1 Introduction

Interactive proof systems have received considerable attention [2,3,4,8,14,10] since their introduction by Babai [1] and Goldwasser, Micali and Rackoff [11] in 1985. An interactive proof system takes the form of a protocol of one or more rounds between two parties, a verifier and a prover. Whereas the prover is computationally unbounded, the verifier is limited to probabilistic polynomial time. Both the prover and the verifier have access to a common input string x. The goal of the prover is to convince the verifier that x belongs to a pre-specified language L. The verifier's aim, on the other hand, is to determine whether the prover's claim is indeed valid. In each round, the verifier sends a polynomial (in x) size query to the prover, who returns a polynomial size answer. At the end of the protocol, the verifier decides to accept, and conclude $x \in L$, or reject based on the messages exchanged and his own private randomness. A language has an interactive proof if there exists a verifier V and a prover P such that: If $x \in L$, the prover can always convince V to accept. If $x \notin L$, no strategy of the prover can convince V to accept with non-negligible probability. IP denotes the class of languages having an interactive proof system. Watrous [30] first considered the notion of *quantum* interactive proof systems. Here, the prover has unbounded quantum computational power whereas the verifier is restricted to quantum polynomial time. In addition, the two parties can now exchange quantum messages. QIP is the class of languages having a quantum interactive proof system. Classically, it is known that IP = PSPACE [22,23]. For the quantum case, it has

* Supported by EU project RESQ IST-2001-37559 and NWO Vici grant 2004-2009.

B. Durand and W. Thomas (Eds.): STACS 2006, LNCS 3884, pp. 162–171, 2006.

been shown that PSPACE $\subseteq$ QIP $\subseteq$ EXP [30,12]. If, in addition, the verifier is given polynomial size quantum advice, the resulting class QIP/qpoly contains all languages [21]. Let QIP(k) denote the class where the prover and verifier are restricted to exchanging k messages. It is known that QIP = QIP(3) [12] and QIP(1) $\subseteq$ PP [29,15]. We refer to [15] for an overview of the extensive work done on QIP(1), also known as QMA. Very little is known about QIP(2) and its relation to either PP or PSPACE.

In multiple-prover interactive proof systems the verifier can interact with multiple, computationally unbounded provers. Before the protocol starts, the provers are allowed to agree on a joint strategy, however they can no longer communicate during the execution of the protocol. Let MIP denote the class of languages having a *multiple*-prover interactive proof system. In this paper, we are especially interested in two-prover interactive proof systems as introduced by Ben-Or, Goldwasser, Kilian and Widgerson [3]. Feige and Lovász [10] have shown that a language is in NEXP if and only if it has a two-prover one-round proof system, i.e. MIP[2] = MIP = NEXP. Let $\oplus$MIP[2] denote the restricted class where the verifier's output is a function of the XOR of two binary answers. Even for such a system $\oplus$MIP[2] = NEXP, for certain soundness and completeness parameters [6]. Classical multiple-prover interactive proof systems are thus more powerful than classical proof systems based on a single prover, assuming PSPACE $\neq$ NEXP. Kobayashi and Matsumoto have considered *quantum* multiple-prover interactive proof systems which form an extension of quantum single prover interactive proof systems as described above. Let QMIP denote the resulting class. In particular, they showed that QMIP = NEXP if the provers do *not* share quantum entanglement. If the provers share at most polynomially many entangled qubits the resulting class is contained in NEXP [13].

Cleve, Høyer, Toner and Watrous [6] have raised the question whether a *classical* two-prover system is weakened when the provers are allowed to share arbitrary entangled states as part of their strategy, but all communication remains classical. We write MIP* if the provers share entanglement. The authors provide a number of examples which demonstrate that the soundness condition of a classical proof system can be compromised, i.e. the interactive proof system is weakened, when entanglement is used. In their paper, it is proved that $\oplus$MIP*[2] $\subseteq$ NEXP. Later, the same authors also showed that $\oplus$MIP*[2] $\subseteq$ EXP using semidefinite programming [7]. Entanglement thus clearly weakens an interactive proof system, assuming EXP $\neq$ NEXP.

Intuitively, entanglement allows the provers to coordinate their answers, even though they cannot use it to communicate. By measuring the shared entangled state the provers can generate correlations which they can use to deceive the verifier. Tsirelson [26,24] has shown that even quantum mechanics limits the strength of such correlations. Consequently, Popescu and Roehrlich [17,18,19] have raised the question why nature imposes such limits. To this end, they constructed a toy-theory based on non-local boxes [17,27], which are hypothetical "machines" generating correlations stronger than possible in nature. In their full generalization, non-local boxes can give rise to any type of correlation as long

as they cannot be used to signal. van Dam has shown that sharing certain non-local boxes allows two remote parties to perform any distributed computation using only a single bit of communication [27,28]. Preda [20] showed that sharing non-local boxes can then allow two provers to coordinate their answers perfectly and obtained $\oplus\text{MIP}_{\text{NL}} = \text{PSPACE}$, where we write $\oplus\text{MIP}_{\text{NL}}$ to indicate that the two provers share non-local boxes.

Kitaev and Watrous [12] mention that it is unlikely that a single-prover *quantum* interactive proof system can simulate multiple classical provers, because then from $\text{QIP} \subseteq \text{EXP}$ and $\text{MIP} = \text{NEXP}$ it follows that $\text{EXP} = \text{NEXP}$.

1.1 Our Contribution

Surprisingly, it turns out that when the provers are allowed to share entanglement it can be possible to simulate two such classical provers by one quantum prover. This indicates that entanglement among provers truly leads to a weaker proof system. In particular, we show that a two-prover one-round interactive proof system where the verifier computes the XOR of two binary answers and the provers are allowed to share an arbitrary entangled state can be simulated by a single quantum interactive proof system with two messages: $\oplus\text{MIP}^*[2] \subseteq \text{QIP}(2)$. Since very little is known about QIP(2) so far [12], we hope that our result may help to shed some light about its relation to PP or PSPACE in the future. Our result also leads to a proof that $\oplus\text{MIP}^*[2] \subseteq \text{EXP}$.

2 Preliminaries

2.1 Quantum Computing

We assume general familiarity with the quantum model [16]. In the following, we will use $\mathcal{V}$,$\mathcal{P}$ and $\mathcal{M}$ to denote the Hilbert spaces of the verifier, the quantum prover and the message space respectively. $\Re(z)$ denotes the real part of a complex number z.

2.2 Non-local Games

For our proof it is necessary to introduce the notion of (non-local) games: Let S, T, A and B be finite sets, and π a probability distribution on $S \times T$. Let V be a predicate on $S \times T \times A \times B$. Then $G = G(V, \pi)$ is the following two-person cooperative game: A pair of questions $(s, t) \in S \times T$ is chosen at random according to the probability distribution π. Then s is sent to player 1, henceforth called Alice, and t to player 2, which we will call Bob. Upon receiving s, Alice has to reply with an answer $a \in A$. Likewise, Bob has to reply to question t with an answer $b \in B$. They win if $V(s, t, a, b) = 1$ and lose otherwise. Alice and Bob may agree on any kind of strategy beforehand, but they are no longer allowed to communicate once they have received questions s and t. The value $\omega(G)$ of a game G is the maximum probability that Alice and Bob win the game. We will follow the approach of Cleve et al. [6] and write $V(a, b|s, t)$ instead of $V(s, t, a, b)$ to emphasize the fact that a and b are answers given questions s and t.

Here, we will be particularly interested in non-local games. Alice and Bob are allowed to share an arbitrary entangled state $|\Psi\rangle$ to help them win the game. Let $\mathcal{A}$ and $\mathcal{B}$ denote the Hilbert spaces of Alice and Bob respectively. The state $|\Psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ is part of the quantum strategy that Alice and Bob can agree on beforehand. This means that for each game, Alice and Bob can choose a specific $|\Psi\rangle$ to maximize their chance of success. In addition, Alice and Bob can agree on quantum measurements. For each $s \in S$, Alice has a projective measurement described by $\{X_s^a : a \in A\}$ on $\mathcal{A}$. For each $t \in T$, Bob has a projective measurement described by $\{Y_t^b : b \in B\}$ on $\mathcal{B}$. For questions $(s,t) \in S \times T$, Alice performs the measurement corresponding to s on her part of $|\Psi\rangle$ which gives her outcome a. Likewise, Bob performs the measurement corresponding to t on his part of $|\Psi\rangle$ with outcome b. Both send their outcome, a and b, back to the verifier. The probability that Alice and Bob answer $(a,b) \in A \times B$ is then given by

$$\langle\Psi|X_s^a \otimes Y_t^b|\Psi\rangle.$$

The probability that Alice and Bob win the game is given by

$$\Pr[\text{Alice and Bob win}] = \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t)\langle\Psi|X_s^a \otimes Y_t^b|\Psi\rangle.$$

The *quantum value* $\omega_q(G)$ of a game G is the maximum probability over all possible quantum strategies that Alice and Bob win. An *XOR game* is a game where the value of V only depends on $c = a \oplus b$ and not on a and b independently. For XOR games we write $V(c|s,t)$ instead of $V(a,b|s,t)$. We will use $\tau(G)$ to denote the value of the trivial strategy where Alice and Bob ignore their inputs and return random answers $a \in_R \{0,1\}$, $b \in_R \{0,1\}$ instead. For an XOR game,

$$\tau(G) = \frac{1}{2} \sum_{s,t} \pi(s,t) \sum_{c \in \{0,1\}} V(c|s,t). \tag{1}$$

In this paper, we will only be interested in the case that $a \in \{0,1\}$ and $b \in \{0,1\}$. Alice and Bob's measurements are then described by $\{X_s^0, X_s^1\}$ for $s \in S$ and $\{Y_t^0, Y_t^1\}$ for $t \in T$ respectively. Note that $X_s^0 + X_s^1 = I$ and $Y_t^0 + Y_t^0 = I$ and thus these measurements can be expressed in the form of observables X_s and Y_t with eigenvalues ± 1: $X_s = X_s^0 - X_s^1$ and $Y_t = Y_t^0 - Y_t^1$. Tsirelson [26,24] has shown that for any $|\Psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ there exists real vectors $x_s, y_t \in \mathbb{R}^N$ with $N = \min(|S|, |T|)$ such that $\langle\Psi|X_s \otimes Y_t|\Psi\rangle = \langle x_s|y_t\rangle$. Conversely, if $dim(\mathcal{A}) = dim(\mathcal{B}) = 2^{\lceil N/2 \rceil}$ and $|\Psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ is a maximally entangled state, there exist observables X_s on $\mathcal{A}$, Y_t on $\mathcal{B}$ such that $\langle x_s|y_t\rangle = \langle\Psi|X_s \otimes Y_t|\Psi\rangle$. See [25, Theorem 3.5] for a detailed construction.

2.3 Interactive Proof Systems

Multiple Provers. It is well known [6,10], that two-prover one-round interactive proof systems with classical communication can be modeled as (non-local) games. Here, Alice and Bob take the role of the two provers. The verifier now

poses questions s and t, and evaluates the resulting answers. A proof system associates with each string x a game G_x, where $\omega_q(G_x)$ determines the probability that the verifier accepts (and thus concludes $x \in L$). The string x, and thus the nature of the game G_x is known to both the verifier and the provers. Ideally, for all $x \in L$ the value of $\omega_q(G_x)$ is close to one, and for $x \notin L$ the value of $\omega_q(G_x)$ is close to zero. It is possible to extend the game model for MIP[2] to use a randomized predicate for the acceptance predicate V. This corresponds to V taking an extra input string chosen at random by the verifier. However, known applications of MIP[2] proof systems do not require this extension [9]. Our argument in Section 3 can easily be extended to deal with randomized predicates. Since V is not a randomized predicate in [6], we here follow this approach.

In this paper, we concentrate on proof systems involving two provers, one round of communication, and single bit answers. The provers are computationally unbounded, but limited by the laws of quantum physics. However, the verifier is probabilistic polynomial time bounded. As defined by Cleve et al. [6],

Definition 1. *For $0 \leq s < c \leq 1$, let $\oplus\mathrm{MIP}_{c,s}[2]$ denote the class of all languages L recognized by a classical two-prover interactive proof system of the following form:*

- *They operate in one round, each prover sends a single bit in response to the verifier's question, and the verifier's decision is a function of the parity of those two bits.*
- *If $x \notin L$ then, whatever strategy the two provers follow, the probability that the verifier accepts is at most s (the* soundness *probability).*
- *If $x \in L$ then there exists a strategy for the provers for which the probability that the verifier accepts is at least c (the* completeness *probability).*

Definition 2. *For $0 \leq s < c \leq 1$, let $\oplus\mathrm{MIP}^*_{c,s}[2]$ denote the class corresponding to a modified version of the previous definition: all communication remains classical, but the provers may share prior quantum entanglement, which may depend on x, and perform quantum measurements.*

A Single Quantum Prover. Instead of two classical provers, we now consider a system consisting of a single quantum prover P_q and a quantum polynomial time verifier V_q as defined by Watrous [30]. Again, the quantum prover P_q is computationally unbounded, however, he is limited by the laws of quantum physics. The verifier and the prover can communicate over a quantum channel. In this paper, we are only interested in one round quantum interactive proof systems: the verifier sends a single quantum message to the prover, who responds with a quantum answer. We here express the definition of QIP(2) [30] in a form similar to the definition of $\oplus\mathrm{MIP}^*$:

Definition 3. *Let $\mathrm{QIP}(2, c, s)$ denote the class of all languages L recognized by a quantum one-prover one-round interactive proof system of the following form:*

- *If $x \notin L$ then, whatever strategy the quantum prover follows, the probability that the quantum verifier accepts is at most s.*

– *If $x \in L$ then there exists a strategy for the quantum prover for which the probability that the verifier accepts is at least c.*

3 Main Result

We now show that an interactive proof system where the verifier is restricted to computing the XOR of two binary answers is in fact no more powerful than a system based on a single quantum prover. The main idea behind our proof is to combine two classical queries into one quantum query, and thereby simulate the classical proof system with a single quantum prover. Recall that the two provers can use an arbitrary entangled state as part of their strategy. For our proof we will make use of the following proposition shown in [6, Proposition 5.7]:

Proposition 1 (CHTW). *Let $G(V, \pi)$ be an XOR game and let $N = min(|S|, |T|)$. Then*

$$w_q(G) - \tau(G) = \frac{1}{2} \max_{x_s, y_t} \sum_{s,t} \pi(s,t) \left(V(0|s,t) - V(1|s,t)\right) \langle x_s | y_t \rangle,$$

where the maximization is taken over unit vectors

$$\{x_s \in \mathbb{R}^N : s \in S\} \cup \{y_t \in \mathbb{R}^N : t \in T\}.$$

Theorem 1. *For all s and c such that $0 \leq s < c \leq 1$, $\oplus\mathrm{MIP}^*_{c,s}[2] \subseteq \mathrm{QIP}(2, c, s)$*

Proof. Let $L \in \oplus\mathrm{MIP}^*_{c,s}[2]$ and let V_e be a verifier witnessing this fact. Let P_e^1 (Alice) and P_e^2 (Bob) denote the two provers sharing entanglement. Fix an input string x. As mentioned above, interactive proof systems can be modeled as games indexed by the string x. It is therefore sufficient to show that there exists a verifier V_q and a quantum prover P_q, such that $w_{sim}(G_x) = w_q(G_x)$, where $w_{sim}(G_x)$ is the value of the simulated game.

Let s,t be the questions that V_e sends to the two provers P_e^1 and P_e^2 in the original game. The new verifier V_q now constructs the following state in $\mathcal{V} \otimes \mathcal{M}$

$$|\Phi_{init}\rangle = \frac{1}{\sqrt{2}}(\underbrace{|0\rangle}_{\mathcal{V}} \underbrace{|0\rangle|s\rangle}_{\mathcal{M}} + \underbrace{|1\rangle}_{\mathcal{V}} \underbrace{|1\rangle|t\rangle}_{\mathcal{M}}),$$

and sends register $\mathcal{M}$ to the single quantum prover P_q[1]

We first consider the honest strategy of the prover. Let a and b denote the answers of the two classical provers to questions s and t respectively. The quantum prover now transforms the state to

$$|\Phi_{honest}\rangle = \frac{1}{\sqrt{2}}((-1)^a \underbrace{|0\rangle}_{\mathcal{V}} \underbrace{|0\rangle|s\rangle}_{\mathcal{M}} + (-1)^b \underbrace{|1\rangle}_{\mathcal{V}} \underbrace{|1\rangle|t\rangle}_{\mathcal{M}}),$$

[1] If questions s and t are always orthogonal, it suffices to use $\frac{1}{\sqrt{2}}(|0\rangle|s\rangle + |1\rangle|t\rangle)$.

and returns register $\mathcal{M}$ back to the verifier. The verifier V_q now performs a measurement on $\mathcal{V} \otimes \mathcal{M}$ described by the following projectors

$$\begin{aligned} P_0 &= |\Psi_{st}^+\rangle\langle\Psi_{st}^+| \otimes I \\ P_1 &= |\Psi_{st}^-\rangle\langle\Psi_{st}^-| \otimes I \\ P_{reject} &= I - P_0 - P_1, \end{aligned}$$

where $|\Psi_{st}^{\pm}\rangle = (|0\rangle|0\rangle|s\rangle \pm |1\rangle|1\rangle|t\rangle)/\sqrt{2}$. If he obtains outcome "reject", he immediately aborts and concludes that the quantum prover is cheating. If he obtains outcome $m \in \{0,1\}$, the verifier concludes that $c = a \oplus b = m$. Note that $\Pr[m = a \oplus b|s,t] = \langle \Phi_{honest}|P_{a\oplus b}|\Phi_{honest}\rangle = 1$, so the verifier can reconstruct the answer perfectly.

We now consider the case of a dishonest prover. In order to convince the verifier, the prover applies a transformation on $\mathcal{M} \otimes \mathcal{P}$ and send register $\mathcal{M}$ back to the verifier. We show that for any such transformation the value of the resulting game is at most $w_q(G_x)$: Note that the state of the total system in $\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ can now be described as

$$|\Phi_{dish}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi_s\rangle + |1\rangle|\phi_t\rangle)$$

where $|\phi_s\rangle = \sum_{u \in S' \cup T'} |u\rangle|\alpha_u^s\rangle$ and $|\phi_t\rangle = \sum_{v \in S' \cup T'} |v\rangle|\alpha_v^t\rangle$ with $S' = \{0s|s \in S\}$ and $T' = \{1t|t \in T\}$. Any transformation employed by the prover can be described this way. We now have that

$$\Pr[m = 0|s,t] = \langle \Phi_{dish}|P_0|\Phi_{dish}\rangle = \frac{1}{4}(\langle\alpha_s^s|\alpha_s^s\rangle + \langle\alpha_t^t|\alpha_t^t\rangle) + \frac{1}{2}\Re(\langle\alpha_s^s|\alpha_t^t\rangle) \quad (2)$$

$$\Pr[m = 1|s,t] = \langle \Phi_{dish}|P_1|\Phi_{dish}\rangle = \frac{1}{4}(\langle\alpha_s^s|\alpha_s^s\rangle + \langle\alpha_t^t|\alpha_t^t\rangle) - \frac{1}{2}\Re(\langle\alpha_s^s|\alpha_t^t\rangle) \quad (3)$$

The probability that the prover wins is given by

$$\Pr[\text{Prover wins}] = \sum_{s,t} \pi(s,t) \sum_{c \in \{0,1\}} V(c|s,t) \Pr[m = c|s,t].$$

The prover will try to maximize his chance of success by maximizing $\Pr[m = 0|s,t]$ or $\Pr[m = 1|s,t]$. We can therefore restrict ourselves to considering real unit vectors for which $\langle\alpha_s^s|\alpha_s^s\rangle = 1$ and $\langle\alpha_t^t|\alpha_t^t\rangle = 1$. This also means that $|\alpha_s^{s'}\rangle = 0$ iff $s \neq s'$ and $|\alpha_t^{t'}\rangle = 0$ iff $t \neq t'$. Any other strategy can lead to rejection and thus to a lower probability of success. By substituting into Equations 2 and 3, it follows that the probability that the quantum prover wins the game when he avoids rejection is then

$$\frac{1}{2} \sum_{s,t,c} \pi(s,t) V(c|s,t)(1 + (-1)^c \langle\alpha_s^s|\alpha_t^t\rangle). \quad (4)$$

In order to convince the verifier, the prover's goal is to choose real vectors $|\alpha_s^s\rangle$ and $|\alpha_t^t\rangle$ which maximize Equation 4. Since in $|\phi_s\rangle$ and $|\phi_t\rangle$ we sum over $|S'| +$

$|T'| = |S|+|T|$ elements respectively, the dimension of $\mathcal{P}$ need not exceed $|S|+|T|$. Thus, it is sufficient to restrict the maximization to vectors in $\mathbb{R}^{|S|+|T|}$. In fact, since we are interested in maximizing the inner product of two vectors from the sets $\{\alpha_s^s : s \in S\}$ and $\{\alpha_t^t : t \in T\}$, it is sufficient to limit the maximization of vectors to $\mathbb{R}^N$ with $N = \min(|S|, |T|)$ [6]: Consider the projection of the vectors $\{\alpha_s^s : s \in S\}$ onto the span of the vectors $\{\alpha_t^t : t \in T\}$ (or vice versa). Given Equation 4, we thus have

$$w_{sim}(G_x) = \max_{\alpha_s^s, \alpha_t^t} \frac{1}{2} \sum_{s,t,c} \pi(s,t) V(c|s,t)(1 + (-1)^c \langle \alpha_s^s | \alpha_t^t \rangle),$$

where the maximization is taken over vectors $\{\alpha_s^s \in \mathbb{R}^N : s \in S\}$, and $\{\alpha_t^t \in \mathbb{R}^N : t \in T\}$. However, Proposition 1 and Equation 1 imply that

$$w_q(G_x) = \max_{x_s, y_t} \frac{1}{2} \sum_{s,t,c} \pi(s,t) V(c|s,t)(1 + (-1)^c \langle x_s | y_t \rangle)$$

where the maximization is taken over unit vectors $\{x_s \in \mathbb{R}^N : s \in S\}$ and $\{y_t \in \mathbb{R}^N : t \in T\}$. We thus have

$$w_{sim}(G_x) = w_q(G_x)$$

which completes our proof.

Corollary 1. *For all s and c such that $0 \leq s < c \leq 1$, $\oplus\mathrm{MIP}^*_{c,s}[2] \subseteq \mathrm{EXP}$.*

Proof. This follows directly from Theorem 1 and the result that $\mathrm{QIP}(2) \subseteq \mathrm{EXP}$ [12].

4 Discussion

It would be interesting to show that this result also holds for a proof system where the verifier is not restricted to computing the XOR of both answers, but some other boolean function. However, it remains unclear what the exact value of a binary game would be. The approach based on vectors from Tsirelson's results does not work for binary games. Whereas it is easy to construct a single quantum query which allows the verifier to compute an arbitrary function of the two binary answers with some advantage, it thus remains unclear how the value of the resulting game is related to the value of a binary game. Furthermore, mere classical tricks trying to obtain the value of a binary function from XOR itself seem to confer extra cheating power to the provers.

Examples of non-local games with longer answers [6], such as the Kochen-Specker or the Magic Square game, seem to make it even easier for the provers to cheat by taking advantage of their entangled state. Furthermore, existing proofs that MIP = NEXP break down if the provers share entanglement. It is therefore an open question whether $\mathrm{MIP}^* = \mathrm{NEXP}$ or, what may be a more likely outcome, $\mathrm{MIP}^* \subseteq \mathrm{EXP}$.

Non-locality experiments between two spacelike separated observers, Alice and Bob, can be cast in the form of non-local games. For example, the experiment based on the well known CHSH inequality [5], is a non-local game with binary answers of which the verifier computes the XOR [6]. Our result implies that this non-local game can be simulated in superposition by a single prover/observer: Any strategy that Alice and Bob might employ in the non-local game can be mirrored by the single prover in the constructed "superposition game", and also vice versa, due to Tsirelson's constructions [26,24] mentioned earlier. This means that the "superposition game" corresponding to the non-local CHSH game is in fact limited by Tsirelson's inequality [26], even though it itself has no non-local character. Whereas this may be purely coincidental, it would be interesting to know its physical interpretation, if any. Perhaps it may be interesting to ask whether Tsirelson type inequalities have any consequences on local computations in general, beyond the scope of these very limited games.

Acknowledgments

Many thanks go to Julia Kempe, Oded Regev and Ronald de Wolf for useful discussions. I would also like to thank Richard Cleve for very useful comments on an earlier draft. Thanks to Daniel Preda for his talk at the CWI seminar [20] about interactive provers using generalized non-local correlations which rekindled my interest in provers sharing entanglement. Many thanks also to Boris Tsirelson for sending me a copy of [24] and [26], and to Falk Unger and Ronald de Wolf for proofreading. Finally, thanks to the anonymous referee whose suggestions helped to improve the presentation of this paper.

References

1. L. Babai. Trading group theory for randomness. In *Proceedings of 17th ACM STOC*, pages 421–429, 1985.
2. L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.
3. M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi prover interactive proofs: How to remove intractability. In *Proceedings of 20th ACM STOC*, pages 113–131, 1988.
4. J. Cai, A. Condon, and R. Lipton. On bounded round multi-prover interactive proof systems. In *Proceedings of the Fifth Annual Conference on Structure in Complexity Theory*, pages 45–54, 1990.
5. J. Clauser, M. Horne, A. Shimony, and R. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.
6. R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of 19th IEEE Conference on Computational Complexity*, pages 236–249, 2004. quant-ph/0404076.
7. R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. Presentation at 19th IEEE Conference on Computational Complexity, 2004.

8. U. Feige. On the success probability of two provers in one-round proof systems. In *Proceedings of the Sixth Annual Conference on Structure in Complexity Theory*, pages 116–123, 1991.
9. U. Feige. Error reduction by parallel repetition - the state of the art. Technical Report CS95-32, Weizmann Institute, 1, 1995.
10. U. Feige and L. Lovász. Two-prover one-round proof systems: their power and their problems. In *Proceedings of 24th ACM STOC*, pages 733–744, 1992.
11. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 1(18):186–208, 1989.
12. A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of 32nd ACM STOC*, pages 608–617, 2000.
13. H. Kobayashi and K. Matsumoto. Quantum Multi-Prover Interactive Proof Systems with Limited Prior Entanglement *J. of Computer and System Sciences*, 66(3):pages 429–450, 2003.
14. D. Lapidot and A. Shamir. Fully parallelized multi prover protocols for NEXP-time. In *Proceedings of 32nd FOCS*, pages 13–18, 1991.
15. C. Marriott and J. Watrous. Quantum Arthur-Merlin games. cs.CC/0506068.
16. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
17. S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.
18. S. Popescu and D. Rohrlich. Nonlocality as an axiom for quantum theory. In *The dilemma of Einstein, Podolsky and Rosen, 60 years later: International symposium in honour of Nathan Rosen*, 1996. quant-ph/9508009.
19. S. Popescu and D. Rohrlich. Causality and nonlocality as axioms for quantum mechanics. In *Proceedings of the Symposium of Causality and Locality in Modern Physics and Astronomy: Open Questions and Possible Solutions*, 1997. quant-ph/9709026.
20. D. Preda. Non-local multi-prover interactive proofs. CWI Seminar, 21 June, 2005.
21. R. Raz. Quantum information and the PCP theorem. quant-ph/0504075. To appear in FOCS 2005.
22. A. Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.
23. A. Shen. IP = PSPACE: simplified proof. *Journal of the ACM*, 39(4):878–880, 1992.
24. B. Tsirelson. Quantum analogues of Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.
25. B. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8(4):329–345, 1993.
26. B. Cirel'son (Tsirelson). Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.
27. W. van Dam. *Nonlocality & Communication Complexity*. PhD thesis, University of Oxford, Department of Physics, 2000.
28. W. van Dam. Impossible consequences of superstrong nonlocality. quant-ph/0501159, 2005.
29. M. Vyalyi. QMA=PP implies that PP contains PH. *Electronic Colloquium on Computational Complexity*, TR03-021, 2003.
30. J. Watrous. PSPACE has constant-round quantum interactive proof systems. In *Proceedings of 40th IEEE FOCS*, pages 112–119, 1999. cs.CC/9901015.