Generalized Tsirelson Inequalities, Commuting-Operator Provers, and Multi-Prover Interactive Proof Systems

Tsuyoshi Ito*
School of Computer Science
McGill University, Montreal, Canada
tsuyoshi@cs.mcgill.ca

Hirotada Kobayashi†
Principles of Informatics Research Division
National Institute of Informatics, Tokyo, Japan
hirotada@nii.ac.jp

Daniel Preda
Computer Science Division
University of California, Berkeley, USA
dpreda@eecs.berkeley.edu

Xiaoming Sun‡
Center for Advanced Study
Tsinghua University, Beijing, China
xiaomings@tsinghua.edu.cn

Andrew C.-C. Yao‡
Center for Advanced Study
Tsinghua University, Beijing, China
andrewcyao@tsinghua.edu.cn

Abstract

A central question in quantum information theory and computational complexity is how powerful nonlocal strategies are in cooperative games with imperfect information, such as multi-prover interactive proof systems. This paper develops a new method for proving limits of nonlocal strategies that make use of prior entanglement among players (or, provers, in the terminology of multi-prover interactive proofs). Instead of proving the limits for usual isolated provers who initially share entanglement, this paper proves the limits for "commuting-operator provers", who share private space, but can apply only such operators that are commutative with any operator applied by other provers. Obviously, these commuting-operator provers are at least as powerful as usual isolated but prior-entangled provers, and thus, limits in the model with commuting-operator provers immediately give limits in the usual model with prior-entangled provers. Using this method, we obtain an n-party generalization of the Tsirelson bound for the Clauser-Horne-Shimony-Holt inequality, for every n. Our bounds are tight in the sense that, in every n-party case, the equality is achievable by a usual nonlocal strategy with prior entanglement. We also apply our method to a three-prover one-round binary interactive proof system for NEXP. Combined with the technique developed by Kempe, Kobayashi, Matsumoto, Toner and Vidick to analyze the soundness of the proof system, it is proved to be NP-hard to distinguish whether the entangled value of a three-prover one-round binary-answer game is equal to one or at most $1 - 1/p(n)$ for some polynomial p, where n is the number of questions. This is in contrast to the two-prover one-round binary-answer case, where the corresponding problem is efficiently decidable. Alternatively, NEXP has a three-prover one-round binary interactive proof system with perfect completeness and soundness $1 - 2^{-\mathrm{poly}}$.

1. Introduction

Nonlocality of multi-party systems is one of the central issues in quantum information theory. This can be naturally expressed within the framework of *nonlocal games* [6], which are cooperative games with imperfect information. Because of this, the nonlocality also has a strong connection with computational complexity theory, in particular with *multi-prover interactive proof systems* [3]. In nonlocal games, the main interests are whether or not the value

of a game changes when parties use nonlocal strategies that make use of prior entanglement, and if it changes, how powerful such nonlocal strategies can be. In multi-prover interactive proof systems, these correspond to the questions if dishonest but prior-entangled provers can break the original soundness condition of the system that is assured for any dishonest classical provers, and if so, how much amount they can deviate from the original soundness condition.

1.1. Our contribution

The main contribution of this paper is to develop a new method for proving limits of nonlocal strategies that make use of prior entanglement among players (or, provers, in the terminology of multi-prover interactive proofs — this paper uses "player" and "prover" interchangeably). Specifically, we consider *commuting-operator provers*, the notion of which was already introduced in the seminal paper by Tsirelson [16]. In contrast to usual provers for multi-prover interactive proofs, commuting-operator provers are no longer isolated, and share a private space corresponding to a Hilbert space $\mathcal{H}$. Initially, they have some state $|\varphi\rangle \in \mathcal{H}$, and when the kth prover P_k receives a question i, he applies some predetermined operation $A_i^{(k)}$ acting over $\mathcal{H}$. The only constraint for the provers is that operators $A_i^{(k)}$ and $A_j^{(l)}$ of different provers P_k and P_l always commute for any questions i and j. It is obvious from this definition that these commuting-operator provers are at least as powerful as usual isolated but prior-entangled provers, and thus, limits in the model with commuting-operator provers immediately give limits in the usual model with prior-entangled provers. Using these commuting-operator provers, or more precisely, making intensive use of the commutative properties of operators, we obtain a number of intriguing results on the limits of nonlocal strategies.

We first show a tight bound of the strategies of commuting-operator players for the generalized $n \times n$ Magic Square game played by n players. This bound is naturally interpreted as an n-party generalization of the Tsirelson bound for the Clauser-Horne-Shimony-Holt (CHSH) inequality, and thus, we essentially obtain a family of generalized Tsirelson-type inequalities, as stated in the following theorem.

Theorem 1. *Let* $X_j^{(i)}$ *be* ±1-*valued observables on* $\mathcal{H}$ *for* $0 \leq i \leq n-1$ *and* $1 \leq j \leq n$ *where* $X_j^{(i)}$ *and* $X_{j'}^{(i')}$ *commute if* $i \neq i'$ ($\forall 1 \leq j, j' \leq n$). *Let* $M_j = \prod_{i=0}^{n-1} X_j^{(i)}$ *and* $N_k = \prod_{i=0}^{n-1} X_{k-i}^{(i)}$ *be observables for* $1 \leq j, k \leq n$, *where the subscript* $k - i$ *is interpreted under modulo* n.

Then,

$$\sum_{j=1}^{n} \langle M_j \rangle + \sum_{k=1}^{n-1} \langle N_k \rangle - \langle N_n \rangle \leq 2n \cos \frac{\pi}{2n}, \quad (1)$$

where $\langle \cdot \rangle$ *denotes expected value.*

In particular, for $n = 2$, our inequality is identical to the Tsirelson bound for the CHSH inequality. For $n = 3$, we have the following corollary, which was originally proved with a different proof in a preliminary work by a subset of the authors (Sun, Yao and Preda [15]).

Corollary 2. *Let* $X_j^{(i)}$ *be* ±1-*valued observables on* $\mathcal{H}$ *for* $1 \leq i, j \leq 3$ *where* $X_j^{(i)}$ *and* $X_{j'}^{(i')}$ *commute if* $i \neq i'$ ($\forall 1 \leq j, j' \leq n$). *Then,*

$$\langle X_1^{(1)} X_1^{(2)} X_1^{(3)} \rangle + \langle X_2^{(1)} X_2^{(2)} X_2^{(3)} \rangle + \langle X_3^{(1)} X_3^{(2)} X_3^{(3)} \rangle$$
$$+ \langle X_1^{(1)} X_3^{(2)} X_2^{(3)} \rangle + \langle X_2^{(1)} X_1^{(2)} X_3^{(3)} \rangle - \langle X_3^{(1)} X_2^{(2)} X_1^{(3)} \rangle$$
$$\leq 3\sqrt{3}.$$

Theorem 1 includes the inequalities proved by Wehner [18] as special cases — our proof is completely different from hers. It is stressed that the inequalities in Theorem 1 and Corollary 2 are tight even in the usual nonlocal model with prior entanglement, a simple proof of which is also given in this paper.

In terms of Magic Square games, Theorem 1 implies the following.

Corollary 3. *For every* $n \geq 2$, *the maximum winning probability in the* n-*player Magic Square game both for commuting-operator players and for usual prior-entangled players is equal to* $(1 + \cos \frac{\pi}{2n})/2$.

Next we prove the limits of the strategies of commuting-operator provers for three-prover one-round interactive proof systems for NP and NEXP. The proof system makes use of three-query non-adaptive probabilistically checkable proof (PCP) systems with perfect completeness due to Håstad [10]. Because of the commutative properties of operators each prover applies, it is quite easy to apply the technique developed by Kempe, Kobayashi, Matsumoto, Toner, and Vidick [11] when analyzing the soundness accepting probability of our system. With this analysis, we show that it is NP-hard to compute the value of a three-player one-round *binary-answer* game with entangled players, which improves the original result in Ref. [11] where a ternary answer from each prover was needed for the NP-hardness. In fact, we show that it is NP-hard even to decide if the value of a three-player one-round binary-answer game is one or not. In sharp contrast to this, the result by Cleve, Høyer, Toner and Watrous [6] implies that the corresponding decision problem is in P in the case with a *two-player* one-round binary-answer game. Alternatively, we

show that any language in NEXP has a three-prover one-round *binary* interactive proof system of perfect completeness with soundness $1 - 2^{\text{poly}}$, whereas only languages in EXP have such proof systems in the two-prover one-round binary case.

More precisely, let $\text{naPCP}_{c(n),s(n)}(r(n), q(n))$ be the class of languages recognized by a probabilistically checkable proof system with completeness and soundness acceptance probabilities $c(n)$ and $s(n)$ such that the verifier uses $r(n)$ random bits and makes $q(n)$ non-adaptive queries, and let $\text{MIP}^*_{c(n),s(n)}(m, 1)$ be the class of languages recognized by a classical m-prover one-round interactive proof system with entangled provers with completeness and soundness acceptance probabilities $c(n)$ and $s(n)$. Our main technical theorem is stated as follows.

Theorem 4. $\text{naPCP}_{1,s(n)}(r(n), 3) \subseteq \text{MIP}^*_{1,1-\varepsilon(n)}(3, 1)$, *where* $\varepsilon(n) = (1/384)(1 - s(n))^2 \cdot 2^{-2r(n)}$. *In this interactive proof system, the verifier uses* $r(n) + O(1)$ *random bits, each prover answers one bit, and honest provers do not need to share prior entanglement. Moreover, the soundness of the interactive proof system holds also against commuting-operator provers.*

By applying Theorem 4 to well-known inclusions $\text{NP} \subseteq \bigcup_{c>0} \text{naPCP}_{1,1-1/n^c}(c \log n, 3)$ and $\text{NEXP} \subseteq \bigcup_{c>0} \text{naPCP}_{1,1-2^{-cn}}(n^c, 3)$, which come from the NP-completeness of the 3SAT problem and the NEXP-completeness of the succinct version of 3SAT (see e.g. Ref. [7]), we obtain the following corollaries.

Corollary 5. *There exists a polynomially bounded function* $p \colon \mathbb{Z}_{\geq 0} \to \mathbb{N}$ *such that, given a classical three-player one-round binary-answer game with n questions with entangled (or commuting-operator) players, it is* NP-*hard to decide whether the value of the game is one or at most* $1 - p(n)$. *Here a game is given as a description of a probability distribution over three-tuples of questions and a table showing whether the answers are accepted or not for each tuple of questions and each tuple of answers.*

Corollary 6. $\text{NP} \subseteq \text{MIP}^*_{1,1-1/\text{poly}}(3, 1)$ *and* $\text{NEXP} \subseteq \text{MIP}^*_{1,1-2^{-\text{poly}}}(3, 1)$, *where the verifier uses* $O(\log n)$ *(resp.* $\text{poly}(n)$*) random bits, each prover answers one bit, and honest provers do not need to share prior entanglement.*

In contrast to Corollaries 5 and 6, the following result in the two-prover case is immediate from the result by Cleve, Høyer, Toner and Watrous [6, Theorem 5.12].

Theorem 7. *(i) Given a classical two-player one-round binary-answer game with entangled players, the problem of deciding whether the value of the game is equal to one or not is in* P.

(ii) Only languages in EXP *have two-prover one-round binary interactive proof systems with entangled*

provers of perfect completeness and soundness acceptance probability $1 - 2^{-\text{poly}}$.

An important consequence of Tsirelson's theorem [16] is that, using semidefinite programming, it is easy to compute the maximum winning probability of a so-called two-player one-round XOR game with entangled players, which is a two-player one-round binary-answer game with entangled players in which the result of the game only depends on the XOR of the answers from the players. Corollary 5 shows that this is not the case if we consider three players and we drop the XOR condition of the game unless $\text{P} = \text{NP}$.

1.2. Background

Multi-prover interactive proof systems (MIPs) were proposed by Ben-Or, Goldwasser, Kilian and Wigderson [3]. It was proved by Babai, Fortnow and Lund [1] that the power of MIPs is exactly equal to NEXP. Subsequently, it was shown that they still achieve NEXP even in the most restrictive setting of two-prover one-round interactive proof systems [8]. One of the main tools when proving these claims is the *oracularization* [3, 9], which forces provers to act just like fixed proof strings.

Cleve, Høyer, Toner and Watrous [6] proved many examples of two-player games where the existence of entanglement increases winning probabilities, including the Magic Square game, which is an example of breakage of the oracularization paradigm under the existence of entanglement. They also proved that two-prover one-round XOR proof systems, or the proof systems where each prover's answer is one bit long and the verifier depends only on the XOR of the answers, recognize NEXP without prior entanglement but at most EXP with prior entanglement.

Kobayashi and Matsumoto [12] showed that multi-prover interactive proof systems with provers sharing at most polynomially many prior-entangled qubits can recognize languages only in NEXP (even if we allow quantum messages between the verifier and each prover). On the other hand, if provers are allowed to share arbitrary many prior-entangled qubits, very little were known about the power of multi-prover interactive proof systems except for the case of XOR proof systems. Very recently, Kempe, Kobayashi, Matsumoto, Toner and Vidick [11] showed that $\text{NP} \subseteq \text{MIP}^*_{1,1-1/\text{poly}}(3, 1)$ and $\text{NEXP} \subseteq \text{MIP}^*_{1,1-2^{-\text{poly}}}(3, 1)$. Cleve, Gavinsky and Jain [5] proved that $\text{NP} \subseteq \oplus\text{MIP}^*_{1-\varepsilon,1/2+\varepsilon}(2, 1)$, where $\oplus\text{MIP}^*_{c(n),s(n)}(2, 1)$ is the class of languages recognized by a two-prover one-round XOR interactive proof system with entangled provers.

The only known relation between the model with commuting-operator provers and the one with usual isolated entangled provers is that they are equivalent in the

two-prover one-round setting that involves only finite-dimensional Hilbert spaces [16, 17].

1.3. Organization of the paper

Section 2 gives definitions on MIP systems used in later sections. Section 3 introduces the commuting-operator-provers model which we will use later and states some basic facts on it. Section 4 discusses the n-player generalization of Tsirelson's bound based on the $n \times n$ Magic Square game. Section 5 treats the three-prover one-round binary interactive proof system for NEXP and compares it with the two-prover case.

2. Preliminaries

We assume basic knowledge about quantum computation, interactive proofs and probabilistically checkable proofs. Readers are referred to textbooks on quantum computation (e.g. Nielsen and Chuang [13]) and on computational complexity (e.g. Du and Ko [7]). Here we review basic notions of multi-prover interactive proof systems that are necessary to define commuting-operator model in Section 3.

A multi-prover interactive proof system can be best viewed as a sequence of cooperative games indexed by input string.

An m-*player cooperative one-round game* (simply an m-*player game* in this paper) is a pair $G = (\pi, V)$ of a probability distribution π over Q^m and a predicate $V : Q^m \times A^m \to \{0, 1\}$, where Q and A are finite sets. As a convention, we denote $V(q_1, \ldots, q_m, a_1, \ldots, a_m)$ by $V(a_1 \cdots a_m \mid q_1 \cdots q_m)$. In this game, a referee decides whether the players win or lose according to a pre-determined rule as follows. The referee chooses questions $q_1, \ldots, q_m$ according to the distribution π and sends the question q_i to the ith player. The ith player sends back an answer $a_i \in A$, and the referee collects the answers $a_1, \ldots, a_m$. The players win if $V(a_1 \cdots a_m \mid q_1 \cdots q_m) = 1$ and lose otherwise. In this paper, we often refer to players as "provers" for better correspondence to multi-prover interactive proof systems.

A *behavior* or a *no-signaling strategy* for G is a function $S : Q^m \times A^m \to [0, 1]$ with normalization and no-signaling conditions. Like V, we denote $S(q_1, \ldots, q_m, a_1, \ldots, a_m)$ by $S(a_1, \ldots, a_m \mid q_1, \ldots, q_m)$, and it corresponds to the probability with which the m players answer $a_1, \ldots, a_m$ under the condition that the questions sent to the players are $q_1, \ldots, q_m$. The *normalization condition* requires that for all $q_1, \ldots, q_m \in Q$, $\sum_{a_1, \ldots, a_m \in A} S(a_1, \ldots, a_m \mid q_1, \ldots, q_m) = 1$. The *no-signaling condition* requires that for any $1 \leq i \leq m$, any $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_m \in Q$ and any $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_m \in A$, the sum $\sum_{a_i \in A} S(a_1, \ldots, a_m \mid q_1, \ldots, q_m)$ does not depend on the choice of $q_i \in Q$. The *winning probability* $w(S)$ of the strategy S is given by

$$w(S) = \sum_{q_1, \ldots, q_m \in Q} \pi(q_1, \ldots, q_m) \times$$

$$\sum_{a_1, \ldots, a_m \in A} S(a_1, \ldots, a_m \mid q_1, \ldots, q_m) V(a_1 \cdots a_m \mid q_1 \cdots q_m).$$

A behavior is said to be *classical* (resp. *entangled*) if it is realized by a classical (resp. entangled) strategy. In a *classical (resp. entangled) strategy*, m computationally unlimited players share a random source (resp. a quantum state), and each of them decides his/her answer according to his/her question and the shared random source (resp. state). It is well-known that for any classical strategy, there exists an equivalent classical strategy without shared random source. Also for any entangled strategy, there exists an equivalent entangled strategy where the players share a pure state and their measurements are projective.

The *classical (resp. entangled, no-signaling) value* of G, denoted by $w_c(G)$ (resp. $w_q(G)$, $w_{ns}(G)$), is the supremum of the winning probabilities over all classical (resp. entangled, no-signaling) behaviors for G. Clearly we have $0 \leq w_c(G) \leq w_q(G) \leq w_{ns}(G) \leq 1$. The classical and no-signaling values of G can be attained for all games G, but it is not known whether the entangled value of G can be attained for all games G.

An m-prover one-round interactive proof system is a pair (M_π, M_V) of two Turing machines. A probabilistic Turing machine M_π is given an input string x and outputs m questions $q_1, \ldots, q_m$. A deterministic Turing machine M_V is given an input x and $2m$ strings $q_1, \ldots, q_m, a_1, \ldots, a_m$, and outputs 0 or 1. Both M_π and M_V must run in time polynomial in $|x|$. This system naturally defines an m-player game G_x for each input string x.

Let $c, s : \mathbb{Z}_{\geq 0} \to [0, 1]$. An m-prover one-round interactive proof system is said to have *completeness acceptance probability* $c(n)$ *for a language* L for classical (resp. entangled) provers when $w_c(G_x) \geq c(|x|)$ (resp. $w_q(G_x) \geq c(|x|)$) for all $x \in L$. Similarly, it is said to have *soundness acceptance probability* $s(n)$ *for a language* L for classical (resp. entangled) provers when $w_c(G_x) \leq s(|x|)$ (resp. $w_q(G_x) \leq s(|x|)$) for all $x \notin L$.

Let $\text{MIP}^*_{c(n), s(n)}(m, 1)$ denote the class of languages having m-prover one-round interactive proof systems with completeness and soundness acceptance probabilities $c(n)$ and $s(n)$ for entangled provers.

Let $\text{naPCP}_{c(n), s(n)}(r(n), q(n))$ denote the class of languages having PCP systems with completeness and soundness acceptance probabilities $c(n)$ and $s(n)$ where the verifier reads $q(n)$ bits of a proof non-adaptively using $r(n)$ random bits.

190

Håstad [10] gave the following characterizations of NP and NEXP.

Theorem 8 (Håstad [10]). *For any constant $3/4 < s < 1$, NP $= \bigcup_{c>0} \mathrm{naPCP}_{1,s}(c \log n, 3)$ and NEXP $= \bigcup_{p \in \mathrm{poly}} \mathrm{naPCP}_{1,s}(p, 3)$.*

It is noted that applying Theorem 4 to the PCP systems in Theorem 8 gives a slightly better soundness in Corollaries 5 and 6 (but polynomials remain polynomials). This is not a significant improvement by itself, but if the soundness bound in Theorem 4 can be improved, then applying it to Theorem 8 will become necessary to obtain a better result on entangled provers.

3. Commuting-operator provers

3.1. Definition and basic properties

Here we define a class of strategies called commuting-operator strategies, which are a generalization of entangled strategies. All the upper bounds of the entangled values of games proved in this paper are actually valid even for this class. A *commuting-operator strategy* is a tuple $(\mathcal{H}, \rho, \mathcal{M}_q^{(i)})$ of a Hilbert space $\mathcal{H}$, a quantum state ρ in $\mathcal{H}$, and a family of POVMs $\mathcal{M}_q^{(i)} = (M_{q,a}^{(i)})_{a \in A}$ on the whole space $\mathcal{H}$ for $1 \leq i \leq m$, $q \in Q$ such that $M_{q,a}^{(i)}$ and $M_{q',a'}^{(i')}$ commute whenever $i \neq i'$: $[M_{q,a}^{(i)}, M_{q',a'}^{(i')}] = M_{q,a}^{(i)} M_{q',a'}^{(i')} - M_{q',a'}^{(i')} M_{q,a}^{(i)} = 0$. In this strategy, m players share a quantum state ρ, and player i measures the state ρ with $\mathcal{M}_{q_i}^{(i)}$ depending on the query q_i sent to him/her. Then the joint probability of the answers $a_1, \ldots, a_m$ under the condition that the questions are $q_1, \ldots, q_m$ is given by $S(a_1, \ldots, a_m \mid q_1, \ldots, q_m) = \operatorname{tr} \rho M_{q_1,a_1}^{(1)} \cdots M_{q_m,a_m}^{(m)}$. Such a behavior S induced by a commuting-operator strategy is called a *commuting-operator behavior*, and the *commuting-operator value* $w_{\mathrm{com}}(G)$ of a game G is the supremum of the winning probabilities over all commuting-operator behaviors for G.

An entangled strategy in the usual sense with Hilbert spaces $\mathcal{H}_1, \ldots, \mathcal{H}_m$ is a special case of commuting-operator strategies with Hilbert spaces $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$, since for $i \neq i'$, POVMs on $\mathcal{H}_i$ and POVMs on $\mathcal{H}_{i'}$ commute element-wise when they are viewed as POVMs on $\mathcal{H}$. This implies that $0 \leq w_{\mathrm{c}}(G) \leq w_{\mathrm{q}}(G) \leq w_{\mathrm{com}}(G) \leq w_{\mathrm{ns}}(G) \leq 1$.

For the special cases of two-player binary-answer games where the referee decides the result of the game depending only on the queries and the XOR of the answers from the two players, the optimal strategy for entangled players and the maximum acceptance probability is given by optimizing certain inner products among vectors [16], and the entangled value of the game can be computed efficiently by using

semidefinite programming. Tsirelson [16] also proved that this value does not change if we replace the entangled players by commuting-operator players. Tsirelson [17] generalized the equivalence of the two models to the case of two players where the dimension of the quantum state shared by the players is finite. However, it is not known whether this equivalence holds for general two-player binary-answer games.

If the outcomes of measurements are real numbers, then the expected values of the product of the outcomes of $\mathcal{M}_{q_i}^{(i)}$ for $i \in P \subseteq \{1, \ldots, m\}$ is $\operatorname{tr} \rho \prod_{i \in P} X_{q_i}^{(i)}$ with observables $X^{(i)} = \sum_{a \in A} a M_{q,a}^{(i)}$.

The following simple observation relates the commutativity of observables and unentangled players.

Lemma 9. *If there is a commuting-operator strategy in a game G with acceptance probability w where all POVM operators $M_{q,a}^{(i)}$ commute, then $w_{\mathrm{c}}(G) \geq w$.*

Proof. Intuitively, the lemma holds since one can measure all the POVMs $\mathcal{M}_q^{(i)}$ simultaneously because of commutativity. Details follow.

Let $a_q^{(i)} \in A$ for $1 \leq i \leq m$ and $q \in Q$, and let $\boldsymbol{a} = (a_1^{(1)}, \ldots, a_{|Q|}^{(1)}, a_1^{(2)}, \ldots, a_{|Q|}^{(2)}, \ldots, a_1^{(m)}, \ldots, a_{|Q|}^{(m)})$. We define a linear operator $M(\boldsymbol{a}) = \prod_{i=1}^{m} \prod_{q \in Q} M_{q, a_q^{(i)}}^{(i)}$. By commutativity of the observables, $M(\boldsymbol{a})$ is Hermitian and nonnegative definite for any $\boldsymbol{a}$, and $\sum_{\boldsymbol{a}} M(\boldsymbol{a}) = I$.

We construct a classical strategy with acceptance probability w. The players share $a_1^{(1)}, \ldots, a_{|Q|}^{(1)}, \ldots, a_1^{(m)}, \ldots, a_{|Q|}^{(m)} \in A$ with probability $\langle \psi | M(\boldsymbol{a}) | \psi \rangle$. The ith player answers $a_q^{(i)}$ when asked query q. By simple calculation, the probability distribution of the answers conditioned on arbitrary set of m queries in the classical strategy is exactly equal to that in the original commuting-operator strategy. $\square$

Like entangled strategies, for any commuting-operator strategy, there exists an equivalent commuting-operator strategy with a pure shared quantum state and projection-valued measures (PVMs).

3.2. Symmetrization

Here we prove that we can assume the players' optimal strategy is symmetric under any permutations of the players. A precise definition of the symmetry of a commuting-operator strategy follows.

Let $G = (\pi, V)$ be an m-player game. G is said to be *symmetric* if the following conditions are satisfied.

(i) π is symmetric: $\pi(q_{\sigma(1)}, \ldots, q_{\sigma(m)}) = \pi(q_1, \ldots, q_m)$ for any permutation $\sigma \in \mathcal{S}_m$.

(ii) V is symmetric under permutations of players: $V(a_{\sigma(1)} \cdots a_{\sigma(m)} \mid q_{\sigma(1)} \cdots q_{\sigma(m)}) = V(a_1 \cdots a_m \mid q_1 \cdots q_m)$ for any permutation $\sigma \in \mathcal{S}_m$.

Now we define the symmetry of a commuting-operator strategy. Let $\mathcal{H}$ be the Hilbert space shared by the players, let $|\Psi\rangle \in \mathcal{H}$ be the state shared by the players, and let $\mathcal{M}_q^{(i)} = (M_{q,a}^{(i)})_{a \in A}$ be the A-valued PVM measured by the player i when asked the question q. The strategy is *symmetric* if there exists a unitary representation Φ of the symmetric group $\mathcal{S}_m$ in $\mathcal{H}$ such that $\Phi(\sigma)|\Psi\rangle = |\Psi\rangle$ and $\Phi(\sigma^{-1})M_{q,a}^{(\sigma(i))}\Phi(\sigma)|\varphi\rangle = M_{q,a}^{(i)}|\varphi\rangle$ for any permutation $\sigma \in \mathcal{S}_m$ and any state $|\varphi\rangle \in \mathcal{H}$.

This definition is a natural extension of the usual definition of symmetric entangled strategy in the following sense: consider an entangled strategy on a Hilbert space $\mathcal{H} = \mathcal{K}^{\otimes m}$, that is, $|\Psi\rangle \in \mathcal{K}^{\otimes n}$ is a state shared by the players and $M_{q,a}^{(i)} = I \otimes \cdots \otimes I \otimes M_{q,a}'^{(i)} \otimes I \otimes \cdots \otimes I$ only acts on the ith tensor factor of $\mathcal{H}$. This strategy is symmetric as a commuting-operator strategy with respect to the representation Φ of $\mathcal{S}_m$ in $\mathcal{H}$ defined by $\Phi(\sigma)(|\varphi_1\rangle \otimes \cdots \otimes |\varphi_m\rangle) = |\varphi_{\sigma^{-1}(1)}\rangle \otimes \cdots \otimes |\varphi_{\sigma^{-1}(m)}\rangle$ if and only if $M_q'^{(1)} = \cdots = M_q'^{(m)}$ for all $q \in Q$.

Lemma 10. *In an m-player one-round symmetric game, if there exists a commuting-operator strategy achieving winning probability p, then there also exists a symmetric commuting-operator strategy achieving the same winning probability p.*

Lemma 10 can be proved by constructing a symmetric strategy by averaging over all the permutations on provers. The proof is omitted due to the space limitation.

4. n-party generalization of Tsirelson's bound based on $n \times n$ Magic Square

4.1. Definitions and basic facts

We define an n-player game for the $n \times n$ Magic Square as follows. Consider an $n \times n$ matrix with $\{0,1\}$-entries not known to the referee. The referee chooses one row or column randomly and uniformly. Then he assigns the n cells on the chosen row or column to the n players one-to-one randomly and uniformly, and queries the content of each cell to the corresponding player. Every player answers either 0 or 1. The players win if and only if the sum of the n answers is even, except that, when the referee chose the column n, the players win if and only if the sum of the n answers is odd. We call this game the n-*player Magic Square game* and denote MS_n.

We consider a variant of this game. Let $L = (L_{jk})$ be a Latin square of order n. That is, $L_{jk} \in \{1, \ldots, n\}$ and

every row or column contains $1, \ldots, n$ exactly once. We define the n-player Magic Square game with assignment L, denoted $\mathrm{MS}_n(L)$, as follows. The referee chooses one row or column randomly and uniformly. Then he queries the contents of the n cells on the chosen row or column to the n players, but this time he assigns the cells to the players according to L: the referee asks the L_{jk}-th player the content of the cell at row j, column k. The rest is the same.

It is easy to verify that $w_\mathrm{c}(\mathrm{MS}_n) = w_\mathrm{c}(\mathrm{MS}_n(L)) = 1 - 1/(2n)$ for any Latin squares L, and this classical bound corresponds to a sequence of Bell inequalities. The Bell inequality corresponding to the two-player Magic Square game with an assignment is known as the Clauser–Horne–Shimony–Holt (CHSH) inequality [4], and the maximum winning probability $w_\mathrm{q}(\mathrm{MS}_2(L)) = w_\mathrm{com}(\mathrm{MS}_2(L)) = (2 + \sqrt{2})/4 \approx 0.85$ for entangled players and even commuting-operator players follows from the quantum version of the CHSH inequality called Tsirelson's bound [16].

The following theorem states that an upper bound for the value of the game $\mathrm{MS}_n(L)$ is also valid for MS_n. This can be proved by a symmetrization argument similar to Lemma 10, and the proof is omitted.

Theorem 11. *For any Latin square L of order n, $w_\mathrm{q}(\mathrm{MS}_n) \leq w_\mathrm{q}(\mathrm{MS}_n(L))$ and $w_\mathrm{com}(\mathrm{MS}_n) \leq w_\mathrm{com}(\mathrm{MS}_n(L))$.*

4.2. A strategy for entangled players

Theorem 12. *There exists an entangled strategy in the n-player Magic Square game with winning probability $(1 + \cos(\pi/(2n)))/2$. That is, $w_\mathrm{q}(\mathrm{MS}_n) \geq (1 + \cos(\pi/(2n)))/2$.*

We define an n-qubit pure state $|\varphi_n\rangle \in (\mathbb{C}^2)^{\otimes n}$ as

$$|\varphi_n\rangle = \frac{1}{2^{(n-1)/2}}\Big(\sum_{\substack{x \in \{0,1\}^n \\ W(x) \equiv 0 \bmod 4}} |x\rangle - \sum_{\substack{x \in \{0,1\}^n \\ W(x) \equiv 2 \bmod 4}} |x\rangle \Big),$$

where $W(x)$ is the number of 1's in $x \in \{0,1\}^n$.

We denote by Z_θ the ± 1-valued observable represented by the 2×2 Hermitian matrix

$$Z_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

The n players share the n-qubit state $|\varphi_n\rangle$, one qubit for each player. When asked the content of the cell at row j, column k, the player measures the observable $Z_{\theta_{jk}}$, where

$$\theta_{jk} = \begin{cases} 0 & \text{if } 1 \leq j, k \leq n-1, \\ \pi/(2n) & \text{if } 1 \leq j \leq n-1, k = n, \\ -\pi/(2n) & \text{if } j = n, 1 \leq k \leq n-1, \\ \pi/2 & \text{if } j = k = n, \end{cases}$$

and answers 0 (resp. 1) if the measured value is $+1$ (resp. -1).

To prove the players win with probability $(1 + \cos(\pi/(2n)))/2$, we use the following lemma, which can be proved by induction on n and a simple calculation. The proof is omitted.

Lemma 13. *Let $n \geq 1$ and $\theta_1, \ldots, \theta_n \in \mathbb{R}$, and let $|\varphi_n\rangle$ and Z_θ as defined above. Let $M = Z_{\theta_1} \otimes \cdots \otimes Z_{\theta_n}$. Then,*

$$\langle \varphi_n | M | \varphi_n \rangle = \cos(\theta_1 + \cdots + \theta_n).$$

It is easy to verify that $\sum_k \theta_{jk} = \pi/(2n)$ for every row j. Similarly, $\sum_j \theta_{jk} = -\pi/(2n)$ for every $k \neq n$, and $\sum_j \theta_{jn} = \pi - \pi/(2n)$. By Lemma 13, the expected value of the product of the n measurement results is $\cos(\pi/(2n))$, except that, when the referee chose the column n, the expected value of the product is $\cos(\pi - \pi/(2n)) = -\cos(\pi/(2n))$. This means that the players win with probability $(1 + \cos\frac{\pi}{2n})/2$ for every query.

4.3. Optimality of the strategy

We prove Theorem 1 and Corollary 3 in this section. We use the following lemma to prove Theorem 1.

Lemma 14. *Let $\mathcal{H}$ be a Hilbert space, $|\varphi\rangle \in \mathcal{H}$ be a unit vector, and A, B be unitary operators on $\mathcal{H}$. (We do not assume that A and B commute.) Let $\alpha = \langle \varphi | A | \varphi \rangle$ and $\beta = \langle \varphi | B | \varphi \rangle$. Then $\left| \langle \varphi | AB | \varphi \rangle - \alpha\beta \right| \leq \sqrt{1 - |\alpha|^2} \sqrt{1 - |\beta|^2}$.*

Proof. If $|\beta| = 1$, then $B|\varphi\rangle = \beta|\varphi\rangle$ and the statement is trivial. In the rest of the proof, we assume that $|\beta| < 1$.

Let $|\psi\rangle = (B|\varphi\rangle - \beta|\varphi\rangle)/\sqrt{1 - |\beta|^2}$. Then $\langle \varphi | \psi \rangle = 0$ and $\langle \psi | \psi \rangle = 1$. It follows that $\langle \varphi | AB | \varphi \rangle = \langle \varphi | A(\beta|\varphi\rangle + \sqrt{1 - |\beta|^2} |\psi\rangle) = \alpha\beta + \langle \varphi | A | \psi \rangle \sqrt{1 - |\beta|^2}$. Let $|\xi\rangle = A^*|\varphi\rangle$. Since $\langle \varphi | \psi \rangle = 0$, we have $\left| \langle \xi | \varphi \rangle \right|^2 + \left| \langle \xi | \psi \rangle \right|^2 \leq 1$. Note that $\langle \xi | \varphi \rangle = \langle \varphi | A | \varphi \rangle = \alpha$. It follows that $\left| \langle \varphi | A | \psi \rangle \right|^2 = \left| \langle \xi | \psi \rangle \right|^2 \leq 1 - |\alpha|^2$. Hence $\left| \langle \varphi | AB | \varphi \rangle - \alpha\beta \right|^2 = \left| \langle \varphi | A | \psi \rangle \right|^2 (1 - |\beta|^2) \leq (1 - |\alpha|^2)(1 - |\beta|^2)$. $\square$

Corollary 15. *Let $\mathcal{H}$, $|\varphi\rangle$, A, B, α and β be as defined in Lemma 14. Suppose $\alpha \in \mathbb{R}$, $\alpha = \cos\theta$, $\Re\beta = \cos\theta'$ with $0 \leq \theta, \theta' \leq \pi$, where $\Re$ denotes the real part. Then $\cos(\theta + \theta') \leq \Re\langle \varphi | AB | \varphi \rangle \leq \cos(\theta - \theta')$.*

Proof. By Lemma 14,

$$\left| \Re\langle \varphi | AB | \varphi \rangle - \alpha\Re(\beta) \right| = \left| \Re(\langle \varphi | AB | \varphi \rangle - \alpha\beta) \right|$$
$$\leq \left| \langle \varphi | AB | \varphi \rangle - \alpha\beta \right| \leq \sqrt{1 - \alpha^2} \sqrt{1 - |\beta|^2}$$
$$\leq \sqrt{1 - \alpha^2} \sqrt{1 - (\Re\beta)^2},$$

which implies

$$\alpha\Re(\beta) - \sqrt{1 - \alpha^2}\sqrt{1 - (\Re\beta)^2} \leq \Re\langle \varphi | AB | \varphi \rangle$$
$$\leq \alpha\Re(\beta) + \sqrt{1 - \alpha^2}\sqrt{1 - (\Re\beta)^2}.$$

The statement follows from the facts that $\alpha = \cos\theta$, $\Re\beta = \cos\theta'$ and $\sin\theta, \sin\theta' \geq 0$. $\square$

Corollary 16. *Let $|\varphi\rangle$ be a unit vector in a Hilbert space $\mathcal{H}$, let $A_1, \ldots, A_n$ be Hermitian operators on $\mathcal{H}$ with $A_i^2 = I$, and let $\langle \varphi | A_i | \varphi \rangle = \cos\theta_i$ with $0 \leq \theta_i \leq \pi$. If $\theta_1 + \cdots + \theta_n < \pi$, then $\Re\langle \varphi | A_1 \cdots A_n | \varphi \rangle \geq \cos(\theta_1 + \cdots + \theta_n) > -1$.*

Proof. Use Corollary 15 repeatedly. $\square$

Proof of Theorem 1. For notational convenience, the index j in $X_j^{(i)}$ is interpreted in modulo n. Let $|\varphi\rangle$ be the quantum state shared by the n parties, and $Z = \sum_{j=1}^n M_j + \sum_{k=1}^{n-1} N_k - N_n$. We prove $\langle Z \rangle = \langle \varphi | Z | \varphi \rangle \leq 2n \cos(\pi/(2n))$.

Let $P = M_1 N_n M_2 N_{n-1} \cdots M_n N_1$. We prove that $P = I$. For $i = 0, \ldots, n-1$, let

$$P_i = \prod_{j=1}^n X_j^{(i)} X_{n+1-j-i}^{(i)}$$
$$= X_1^{(i)} X_{n-i}^{(i)} X_2^{(i)} X_{n-1-i}^{(i)} \cdots X_n^{(i)} X_{1-i}^{(i)}.$$

Note that $P = P_0 P_1 \cdots P_{n-1}$, since $X_j^{(i)}$ and $X_{j'}^{(i')}$ commute whenever $i \neq i'$ by assumption.

Fix any i with $0 \leq i \leq n-1$. We define $Y_{2j-1} = X_j^{(i)}$ and $Y_{2j} = X_{n+1-j-i}^{(i)}$. Note that $P_i = Y_1 Y_2 \cdots Y_{2n}$. By calculation, it can be verified that $Y_{n-i+1-k} = Y_{n-i+k}$ for $1 \leq k \leq n-i$. Since $Y_j^2 = I$ for all $1 \leq j \leq 2n$, this implies that $Y_1 Y_2 \cdots Y_{2(n-i)} = Y_1(Y_2 \cdots (Y_{n-i} Y_{n-i+1}) \cdots Y_{2(n-i)-1}) Y_{2(n-i)} = I$. Similarly, the equation $Y_{2n-i+1-k} = Y_{2n-i+k}$ for $1 \leq k \leq i$ implies that $Y_{2(n-i)+1} \cdots Y_{2n} = I$. Therefore $P_i = (Y_1 \cdots Y_{2(n-i)})(Y_{2(n-i)+1} \cdots Y_{2n}) = I$. This concludes that $P = P_0 \cdots P_{n-1} = I$.

Let $\langle \varphi | M_j | \varphi \rangle = \cos\theta_j$ for $1 \leq j \leq n$, $\langle \varphi | N_k | \varphi \rangle = \cos\theta_k'$ for $1 \leq k \leq n-1$, and $-\langle \varphi | N_n | \varphi \rangle = \cos\theta_n'$ with $0 \leq \theta_j, \theta_k' \leq \pi$. Since $M_1(-N_n)M_2 N_{n-1} M_3 N_{n-2} \cdots M_n N_1 = -P = -I$, it holds that $\sum_{j=1}^n \theta_j + \sum_{k=1}^n \theta_k' \geq \pi$ by Corollary 16. As is shown in the following Lemma 17, $\langle \varphi | Z | \varphi \rangle \leq 2n \cos(\pi/(2n))$ subject to this constraint, which establishes Theorem 1. $\square$

Lemma 17. *Let $n \geq 1$, $0 \leq \theta_1, \ldots, \theta_n \leq \pi$ and $\theta_1 + \cdots + \theta_n \geq \pi$. Then $\cos\theta_1 + \cdots + \cos\theta_n \leq n \cos(\pi/n)$.*

Proof. Since the function $\cos\theta$ is decreasing in the range $0 \leq \theta \leq \pi$, we may assume that $\theta_1 + \cdots + \theta_n = \pi$. The

193

statement is trivial for $n \leq 2$. We assume $n \geq 3$ for the rest of the proof.

First consider the case where $0 \leq \theta_1, \ldots, \theta_n \leq \pi/2$. In this case, since the function $\cos\theta$ is concave in the range $0 \leq \theta \leq \pi/2$, it follows that $\cos\theta_1 + \cdots + \cos\theta_n \leq n\cos(\pi/n)$.

Next consider the case where for some i, $\theta_i > \pi/2$. Without loss of generality, we assume that $\theta_1 > \pi/2$. Then, again from the concavity of the function $\cos\theta$ in the range $0 \leq \theta \leq \pi/2$, it follows that $\cos\theta_2 + \cdots + \cos\theta_n \leq (n-1)\cos((\pi-\theta_1)/(n-1))$. Since $\cos\theta_1 + (n-1)\cos((\pi-\theta_1)/(n-1))$ is decreasing in the range $\pi/2 \leq \theta_1 \leq \pi$,

$$\cos\theta_1 + \cdots + \cos\theta_n$$
$$\leq \cos\theta_1 + (n-1)\cos\frac{\pi-\theta_1}{n-1}$$
$$< \cos\frac{\pi}{2} + (n-1)\cos\frac{\pi}{2(n-1)} < n\cos\frac{\pi}{n}. \qquad \square$$

To prove Corollary 3, we consider the n-player Magic Square game with the assignment L defined as $L = (L_{jk})$ with $L_{jk} \equiv k - j \bmod n$. We refer to this Latin square as the cyclic Latin square of order n, and this game as the n-player Magic Square game with the cyclic assignment.

Proof of Corollary 3. Note that the inequality (1) is equivalent to the claim that $w_{\mathrm{com}}(\mathrm{MS}_n(L)) \leq (1 + \cos\frac{\pi}{2n})/2$ for the cyclic Latin square L. Therefore, Corollary 3 follows from Theorems 1, 11 and 12. $\qquad \square$

We note that Theorem 1 includes the following inequality proved by Wehner [18] as special cases.

Theorem 18 (Wehner [18]). *Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be a Hilbert space consisting of two subsystems, and let $|\varphi\rangle \in \mathcal{H}$ be a state. Let $n \geq 1$, and let $X_1, \ldots, X_n$ be ±1-valued observables on $\mathcal{H}_1$ and $Y_1, \ldots, Y_n$ be ±1-valued observables on $\mathcal{H}_2$. Then,*

$$\sum_{j=1}^{n}\langle X_j Y_j\rangle + \sum_{j=1}^{n-1}\langle X_{j+1}Y_j\rangle - \langle X_1 Y_n\rangle \leq 2n\cos\frac{\pi}{2n}. \quad (2)$$

Proof. In the inequality (1), let $X_j^{(0)} = I \otimes Y_j$, $X_j^{(n-1)} = X_j \otimes I$, and $X_j^{(i)} = I \otimes I$ for $1 \leq i \leq n-2$. Then the inequality (1) is exactly the same as the inequality (2). $\qquad \square$

The equality in (2) is achievable [14]. This gives another proof of $w_{\mathrm{q}}(\mathrm{MS}_n(L)) \geq (1+\cos\frac{\pi}{2n})/2$ for the cyclic Latin square L (but not of $w_{\mathrm{q}}(\mathrm{MS}_n) \geq (1 + \cos\frac{\pi}{2n})/2$).

Remark 1. For some games G, an upper bound on $w_{\mathrm{q}}(G)$ is obtained from an upper bound on the no-signaling value $w_{\mathrm{ns}}(G)$ of G, which can be characterized by linear programming and often easier to compute than $w_{\mathrm{q}}(G)$. This is not the case for Corollary 3 since $w_{\mathrm{ns}}(\mathrm{MS}_n) = 1$. This follows from the result by Barrett and Pironio [2, Theorem 1]: for any game $G = (\pi, V)$ where the predicate V does not depend on the individual answers from the players but only on the XOR of all the answers, there exists a no-signaling strategy with winning probability one.

Remark 2. We say two Latin squares of order n are equivalent if one is obtained from the other by swapping rows, swapping columns, relabelling the elements, and/or transposing. For $n \geq 4$, Latin squares of order n is not unique up to this symmetry. For $n = 4$, there are two inequivalent Latin squares:

$$L = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\\hline 4 & 1 & 2 & 3 \\\hline 3 & 4 & 1 & 2 \\\hline 2 & 3 & 4 & 1 \\\hline\end{array}, \qquad L' = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\\hline 2 & 1 & 4 & 3 \\\hline 3 & 4 & 1 & 2 \\\hline 4 & 3 & 2 & 1 \\\hline\end{array}.$$

The first Latin square L is cyclic, but the second Latin square L' is not. The proof of Corollary 3 depends on the actual assignment of cells to the provers and it is not applicable to L'. It can be verified by exhaustive search that for L', the product of the matrices $M_1, M_2, M_3, M_4, N_1, N_2, N_3, N_4$ in any order where each of the eight matrices appears exactly once is not equal to $-I$ for general matrices A_{jk}.

5. Three-prover proof system based on three-query PCP

5.1. Construction of proof system

Let $L \in \mathrm{naPCP}_{1,s(n)}(r(n), 3)$. We construct a three-prover one-round interactive proof system for L as follows. First, the verifier acts like the PCP verifier except that, instead of reading the q_1th, q_2th and q_3th bits of the proof, he writes down the three numbers q_1, q_2, q_3. Next, he performs either *consistency test* or *PCP simulation test* each with probability $1/2$. In the consistency test, the verifier chooses $q \in \{q_1, q_2, q_3\}$ each with probability $1/3$, and sends q to the three provers. He accepts if and only if the three answers coincide. In the PCP simulation test, he sends q_1, q_2, q_3 to the three different provers randomly. He interprets the answers from the provers as the q_1th, q_2th and q_3th bits in the proof, and accepts or rejects just as the PCP verifier would do.

This interactive proof system clearly achieves perfect completeness with honest provers answering the asked bit in the proof. In the rest of this section, we will show that the soundness acceptance probability of this interactive proof system with any commuting-operator provers is at most $1 - (1/384)(1 - s(n))^2 \cdot 2^{-2r(n)}$.

194

Our soundness analysis to prove Theorem 4 shows that for any commuting-operator strategy with high acceptance probability, there exists a cheating proof string for the underlying PCP system. The construction of the cheating proof string is similar to the construction of unentangled strategy used in [11].

We note that without the consistency test, the entangled provers can sometimes cheat with certainty. An example is the well-known GHZ-game, which corresponds to an unsatisfiable boolean formula $f = (x_1 \oplus x_3 \oplus x_5) \wedge (\overline{x_1 \oplus x_4 \oplus x_6}) \wedge (x_2 \oplus x_3 \oplus x_6) \wedge (\overline{x_2 \oplus x_4 \oplus x_5})$, where $\oplus$ denotes the exclusive OR.

5.2. Impossibility of perfect cheating

Before proceeding to the proof of Theorem 4, we first give a much simpler proof of the fact that entangled or even commuting-operator provers cannot cheat with certainty in the interactive proof system constructed in the previous subsection if $x \notin L$. Such impossibility of perfect cheating was originally proved in a preliminary work by Sun, Yao and Preda [15] with a different proof. This paper gives a simpler proof of this fact.

Assume that there exists a commuting-operator strategy for perfect cheating. We prove that such a strategy essentially satisfies the condition stated in Lemma 9. Precisely speaking, we define a "good" subspace $\mathcal{H}'$ of $\mathcal{H}$ containing the shared quantum state such that the restrictions of the POVM operators to $\mathcal{H}'$ pairwise commute.

Let $|\Psi\rangle \in \mathcal{H}$ be the state shared by the three provers, and $\mathcal{M}_q^{(i)} = (M_{q,a}^{(i)})_{a \in \{0,1\}}$ be the PVM measured by prover i for question q. Because the strategy by the provers is accepted with certainty, it must pass the consistency test in particular. This means that $\langle \Psi | M_{q,0}^{(i)} M_{q,0}^{(i')} | \Psi \rangle + \langle \Psi | M_{q,1}^{(i)} M_{q,1}^{(i')} | \Psi \rangle = 1$ for $i \neq i'$ and all $q \in Q$, or equivalently,

$$M_{q,a}^{(1)} |\Psi\rangle = M_{q,a}^{(2)} |\Psi\rangle = M_{q,a}^{(3)} |\Psi\rangle \tag{3}$$

for all $q \in Q$ and $a \in \{0,1\}$.

Let $\mathcal{H}'$ be the subspace of $\mathcal{H}$ spanned by vectors obtained from $|\Psi\rangle$ by applying zero or more of $M_{q,a}^{(i)}$ for any times and in any order.

Claim 1. If $|\varphi\rangle \in \mathcal{H}'$, then $M_{q,a}^{(1)} |\varphi\rangle = M_{q,a}^{(2)} |\varphi\rangle = M_{q,a}^{(3)} |\varphi\rangle$.

Proof. The proof is by induction on the number k of operators applied to $|\Psi\rangle$ to obtain $|\varphi\rangle$.

The case of $k = 0$ is by assumption. If $k > 0$, then $|\varphi\rangle = M |\xi\rangle$ with $M \in \{M_{q',a'}^{(1)}, M_{q',a'}^{(2)}, M_{q',a'}^{(3)}\}$ for some q' and a', and $|\xi\rangle$ is obtained by applying $M_{q,a}^{(i)}$ for $k-1$ times to $|\Psi\rangle$. By the induction hypothesis, $|\varphi\rangle = M_{q',a'}^{(1)} |\xi\rangle = M_{q',a'}^{(2)} |\xi\rangle = M_{q',a'}^{(3)} |\xi\rangle$. Therefore, $M_{q,a}^{(1)} |\varphi\rangle = M_{q,a}^{(2)} |\varphi\rangle$

since $M_{q,a}^{(1)} |\varphi\rangle = M_{q,a}^{(1)} M_{q',a'}^{(3)} |\xi\rangle = M_{q',a'}^{(3)} M_{q,a}^{(1)} |\xi\rangle = M_{q',a'}^{(3)} M_{q,a}^{(2)} |\xi\rangle = M_{q,a}^{(2)} M_{q',a'}^{(3)} |\xi\rangle = M_{q,a}^{(2)} |\varphi\rangle$, here we use the fact that $M_{q,a}^{(i)}$ and $M_{q',a'}^{(i')}$ commute whenever $i \neq i'$. The equation $M_{q,a}^{(2)} |\varphi\rangle = M_{q,a}^{(3)} |\varphi\rangle$ is proved similarly. $\square$

Claim 2. The $6n$ projectors $M_{q,a}^{(i)}$ pairwise commute on $\mathcal{H}'$.

Proof. Let $|\varphi\rangle \in \mathcal{H}'$. By Claim 1, $M_{q,a}^{(1)} M_{q',a'}^{(1)} |\varphi\rangle = M_{q,a}^{(1)} M_{q',a'}^{(3)} |\varphi\rangle = M_{q',a'}^{(3)} M_{q,a}^{(1)} |\varphi\rangle = M_{q',a'}^{(3)} M_{q,a}^{(2)} |\varphi\rangle = M_{q,a}^{(2)} M_{q',a'}^{(3)} |\varphi\rangle = M_{q,a}^{(2)} M_{q',a'}^{(1)} |\varphi\rangle = M_{q',a'}^{(1)} M_{q,a}^{(2)} |\varphi\rangle = M_{q',a'}^{(1)} M_{q,a}^{(1)} |\varphi\rangle$. The equations $M_{q,a}^{(2)} M_{q',a'}^{(2)} |\varphi\rangle = M_{q',a'}^{(2)} M_{q,a}^{(2)} |\varphi\rangle$ and $M_{q,a}^{(3)} M_{q',a'}^{(3)} |\varphi\rangle = M_{q',a'}^{(3)} M_{q,a}^{(3)} |\varphi\rangle$ are proved similarly. $\square$

Note that $|\Psi\rangle \in \mathcal{H}'$ and that $\mathcal{H}'$ is invariant under each $M_{q,a}^{(i)}$. This means that we could use $\mathcal{H}'$ instead of $\mathcal{H}$ in the first place. By Claim 2, these $6n$ operators are pairwise commuting Hermitian operators when restricted to $\mathcal{H}'$. By Lemma 9, there exists a classical strategy achieving the same acceptance probability 1, and therefore the original PCP is accepted with certainty. This means that if $x \notin L$, the commuting-operator provers cannot achieve perfect cheating.

Remark 3. A statement analogous to Claim 2 does not hold if there are only two provers. For example, let $|\Psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2} \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Let M_1, M_2 be arbitrary Hermitian projectors on $\mathbb{C}^2$ such that M_1 and M_2 do not commute, and let $M_{q,1}^{(1)} = M_q \otimes I$, $M_{q,1}^{(2)} = I \otimes (I - M_q)$ for $q = 1, 2$. Then $M_{q,a}^{(1)} |\Psi\rangle = M_{q,a}^{(2)} |\Psi\rangle$ for $q \in \{1, 2\}$ and $a \in \{0, 1\}$ whereas $M_{1,a}^{(1)} M_{2,a'}^{(1)} |\Psi\rangle \neq M_{2,a'}^{(1)} M_{1,a}^{(1)} |\Psi\rangle$.

5.3. Proof of Theorem 4

In the case of imperfect cheating, the equalities in (3) hold only approximately, and we cannot define a "good" subspace $\mathcal{H}'$ as in the case of perfect cheating. Instead, we will prove that an approximate version of the equation (3) implies that measurements $\mathcal{M}_q^{(i)}$ are almost commuting on the shared state $|\Psi\rangle$.

Kempe, Kobayashi, Matsumoto, Toner and Vidick [11] prove soundness of their classical three-prover interactive proof system by comparing the behavior of the first and second provers in an arbitrary entangled strategy to that in the strategy modified as follows: instead of measuring the answer to the asked question, the two provers always measure the answers to all possible questions and just send back the answer to the asked question. This modification makes the behavior classical. The key in their proof is that if the third prover answers consistently with high probability, the measurements performed by the first and second provers do not

195

disturb the reduced state shared by them so much (Claim 20 in [11]), and the modification above does not decrease the acceptance probability so much.

We will use a similar idea when constructing a proof string for the original PCP system, but instead of the non-disturbance property, we use the fact that all the POVMs almost commute on $|\Psi\rangle$. This modification of the proof technique seems necessary because taking partial trace is meaningless in the commuting-operator model.

The following lemma is the key to bound the difference between two POVMs applied to states other than $|\Psi\rangle$. The proof is easy but tedious and omitted.

Lemma 19. *Let ρ be a density matrix, and $\mathcal{M} = (M_i)_{i=1}^v$ and $\mathcal{N} = (N_i)_{i=1}^v$ be POVMs. Let*

$$\lambda = \frac{1}{2}\sum_{i=1}^v \mathrm{tr}\,\rho(\sqrt{M_i} - \sqrt{N_i})^2$$

$$= 1 - \sum_{i=1}^v \mathrm{tr}\,\rho\frac{\sqrt{M_i}\sqrt{N_i} + \sqrt{N_i}\sqrt{M_i}}{2},$$

$$\Delta = \sum_{i=1}^v \left\| \sqrt{M_i}\rho\sqrt{M_i} - \sqrt{N_i}\rho\sqrt{N_i} \right\|_{\mathrm{tr}}.$$

Then $\Delta \leq 2\sqrt{2\lambda}$.

We fix an input $x \notin L$. Let $Q \subseteq \mathbb{Z}_{>0}$ be the set of indices of the bits in a proof string which are queried by the PCP verifier with nonzero probability, and N be the maximum of the elements of Q. Note that $|Q| \leq 3 \cdot 2^r$. Let $\pi(q_1, q_2, q_3)$ be the probability with which the PCP verifier reads the q_1th, q_2th and q_3th bits in the proof at the same time ($\sum_{q_1, q_2, q_3 \in Q} \pi(q_1, q_2, q_3) = 1$). Without loss of generality, we assume that $\pi(q_1, q_2, q_3)$ is symmetric and that $\pi(q_1, q_2, q_3) = 0$ if q_1, q_2, q_3 are not all distinct. For $q_1, q_2, q_3 \in Q$ and $a_1, a_2, a_3 \in \{0, 1\}$, let $V(a_1 a_2 a_3 \mid q_1 q_2 q_3) = 1$ if the PCP verifier accepts when he asks the q_1th, q_2th and q_3th bits in the proof and receives the corresponding answers a_1, a_2 and a_3, and $V(a_1 a_2 a_3 \mid q_1 q_2 q_3) = 0$ otherwise. For $q \in Q$, let $\pi_q = \sum_{q_2, q_3 \in Q} \pi(q, q_2, q_3) = \sum_{q_1, q_3 \in Q} \pi(q_1, q, q_3) = \sum_{q_1, q_2 \in Q} \pi(q_1, q_2, q)$. For simplicity, we let $\pi_q = 0$ for $q \notin Q$.

Consider an arbitrary commuting-operator strategy for the constructed three-prover one-round interactive proof system, and let w be its acceptance probability. By Lemma 10, we can assume that this strategy is symmetric without loss of generality. Let $|\Psi\rangle$ be the quantum state shared by the provers. For $1 \leq i \leq 3$ and $q \in Q$, let $\mathcal{M}_q^{(i)} = (M_{q,0}^{(i)}, M_{q,1}^{(i)})$ be the PVM measured by the ith prover when asked the qth bit in the proof. For simplicity, we let $M_{q,0}^{(i)} = I$ and $M_{q,1}^{(i)} = 0$ for $q \notin Q$. Then, when asked the q_1th, q_2th and q_3th bits in the proof, the provers answer $a_1, a_2, a_3 \in \{0, 1\}$ with probability

$$P_{\mathrm{com}}(a_1 a_2 a_3 \mid q_1 q_2 q_3) = \left\| M_{q_1,a_1}^{(1)} M_{q_2,a_2}^{(2)} M_{q_3,a_3}^{(3)} |\Psi\rangle \right\|^2.$$

Because the strategy is symmetric, it holds that $\langle\Psi| M_{q,a}^{(1)} M_{q,a}^{(2)} |\Psi\rangle = \langle\Psi| M_{q,a}^{(2)} M_{q,a}^{(3)} |\Psi\rangle = \langle\Psi| M_{q,a}^{(3)} M_{q,a}^{(1)} |\Psi\rangle$. Let

$$\lambda_q = 1 - \sum_{a \in \{0,1\}} \langle\Psi| M_{q,a}^{(1)} M_{q,a}^{(2)} |\Psi\rangle$$

$$= 1 - \sum_{a \in \{0,1\}} \langle\Psi| M_{q,a}^{(2)} M_{q,a}^{(3)} |\Psi\rangle$$

$$= 1 - \sum_{a \in \{0,1\}} \langle\Psi| M_{q,a}^{(3)} M_{q,a}^{(1)} |\Psi\rangle.$$

Note that $\lambda_q = 0$ for $q \notin Q$. Now we can write w as $w = (w_{\mathrm{cons}} + w_{\mathrm{sim}})/2$, where

$$w_{\mathrm{cons}}$$
$$= \sum_{q \in Q} \pi_q \big(P_{\mathrm{com}}(000 \mid qqq) + P_{\mathrm{com}}(111 \mid qqq)\big)$$
$$= \sum_{q \in Q} \pi_q \big(\langle\Psi| M_{q,0}^{(1)} M_{q,0}^{(2)} M_{q,0}^{(3)} |\Psi\rangle + \langle\Psi| M_{q,1}^{(1)} M_{q,1}^{(2)} M_{q,1}^{(3)} |\Psi\rangle\big)$$
$$= \sum_{q \in Q} \pi_q \cdot \frac{1}{2}\bigg(\sum_{a \in \{0,1\}} \big(\langle\Psi| M_{q,a}^{(1)} M_{q,a}^{(2)} |\Psi\rangle + \langle\Psi| M_{q,a}^{(2)} M_{q,a}^{(3)} |\Psi\rangle$$
$$+ \langle\Psi| M_{q,a}^{(3)} M_{q,a}^{(1)} |\Psi\rangle\big) - 1\bigg)$$
$$= 1 - \frac{3}{2}\sum_{q \in Q} \pi_q \lambda_q,$$

$$w_{\mathrm{sim}}$$
$$= \sum_{q_1, q_2, q_3 \in Q} \pi(q_1, q_2, q_3) \times$$
$$\sum_{a_1, a_2, a_3 \in \{0,1\}} P_{\mathrm{com}}(a_1 a_2 a_3 \mid q_1 q_2 q_3) V(a_1 a_2 a_3 \mid q_1 q_2 q_3).$$

Since $\pi_q \geq 1/(3 \cdot 2^r)$ for all $q \in Q$, we have

$$w_{\mathrm{cons}} \leq 1 - \frac{1}{2 \cdot 2^r}\sum_{q \in Q} \lambda_q. \tag{4}$$

We construct a random proof string $y = y_1 \cdots y_N$ according to the probability distribution

$$\Pr(y_1, \ldots, y_N) = \left\| M_{N,y_N}^{(i)} \cdots M_{1,y_1}^{(i)} |\Psi\rangle \right\|^2.$$

Note that the value of the right-hand side does not depend on the choice of i because of the symmetry. For distinct $q_1, q_2, q_3 \in Q$ and for $a_1, a_2, a_3 \in \{0, 1\}$, the joint probability of the events $y_{q_1} = a_1$, $y_{q_2} = a_2$, $y_{q_3} = a_3$ is given by

$$P_{\mathrm{c}}(a_1 a_2 a_3 \mid q_1 q_2 q_3) = \sum_{\substack{y \in \{0,1\}^N \\ y_{q_i} = a_i \,(i=1,2,3)}} \Pr(y_1, \ldots, y_N).$$

196

By the soundness condition of the PCP system,

$$\sum_{q_1,q_2,q_3\in Q}\pi(q_1,q_2,q_3)\times$$
$$\sum_{a_1,a_2,a_3\in\{0,1\}}P_{\mathrm{c}}(a_1a_2a_3\mid q_1q_2q_3)V(a_1a_2a_3\mid q_1q_2q_3)\le s.$$

We will prove that if w_{cons} is large, then the difference between P_{com} and P_{c} is not large and therefore w_{sim} is not much larger than s.

For $a_1,a_2,a_3\in\{0,1\}$ and distinct $q_1,q_2,q_3\in Q$, let

$$P'(a_1a_2a_3\mid q_1q_2q_3)=\|M^{(i)}_{q'_1,a'_1}M^{(i)}_{q'_2,a'_2}M^{(i)}_{q'_3,a'_3}|\Psi\rangle\|^2,$$

where $\{(a'_1,q'_1),(a'_2,q'_2),(a'_3,q'_3)\}=\{(a_1,q_1),(a_2,q_2),(a_3,q_3)\}$ and $q'_1<q'_2<q'_3$. Again the value of the right-hand side does not depend on the choice of i.

Claim 1. *For distinct $q_1,q_2,q_3\in Q$,*

$$\sum_{a_1,a_2,a_3\in\{0,1\}}|P_{\mathrm{c}}(a_1a_2a_3\mid q_1q_2q_3)$$
$$-P'(a_1a_2a_3\mid q_1q_2q_3)|\le\sum_{q=1}^{\max\{q_1,q_2,q_3\}}2\sqrt{2\lambda_q}.$$

Proof. We may assume without loss of generality that $1\le q_1<q_2<q_3\le N$. Let $l=q_3$. We prove the claim by hybrid argument. To do this, we shall define probability distributions $p_0,\dots,p_l$ on $\{0,1\}^l$ such that p_0 and p_l are related to P_{c} and P', respectively. For $1\le q\le l$, we define i_q as $i_q=1$ if $q\in\{q_1,q_2,q_3\}$ and $i_q=2$ otherwise. Note that $M^{(i_q)}_{q,a}$ commutes with $M^{(3)}_{q',a'}$ for all $1\le q'\le l$ and $a'\in\{0,1\}$ in either case.[1] For $0\le q\le l$ and $y\in\{0,1\}^l$, let

$$p_q(y)=\|M^{(i_1)}_{1,y_1}M^{(i_2)}_{2,y_2}\cdots M^{(i_q)}_{q,y_q}\times$$
$$M^{(3)}_{l,y_l}M^{(3)}_{l-1,y_{l-1}}\cdots M^{(3)}_{q+1,y_{q+1}}|\Psi\rangle\|^2.$$

For $a_1,a_2,a_3\in\{0,1\}$,

$$\sum_{\substack{y\in\{0,1\}^l\\ y_{q_i}=a_i\ (i=1,2,3)}}p_0(y)=P_{\mathrm{c}}(a_1a_2a_3\mid q_1q_2q_3),$$

$$\sum_{\substack{y\in\{0,1\}^l\\ y_{q_i}=a_i\ (i=1,2,3)}}p_l(y)=\|M^{(1)}_{q_1,a_1}M^{(1)}_{q_2,a_2}M^{(1)}_{q_3,a_3}|\Psi\rangle\|^2$$
$$=P'(a_1a_2a_3\mid q_1q_2q_3).$$

Let $1\le q\le l$. By Lemma 19, we have

$$\sum_{y_q\in\{0,1\}}\left\|M^{(3)}_{q,y_q}|\Psi\rangle\langle\Psi|M^{(3)}_{q,y_q}-M^{(i_q)}_{q,y_q}|\Psi\rangle\langle\Psi|M^{(i_q)}_{q,y_q}\right\|_{\mathrm{tr}}$$
$$\le 2\sqrt{2\lambda_q}.$$

---
[1] This argument is the reason why we need three provers.

Since the trace distance between two states is an upper bound on the statistical difference between the probability distributions resulting from making the same measurement on the two states,

$$\sum_{y\in\{0,1\}^l}\big|\|M^{(i_1)}_{1,y_1}\cdots M^{(i_{q-1})}_{q-1,y_{q-1}}M^{(3)}_{l,y_l}\cdots M^{(3)}_{q+1,y_{q+1}}M^{(3)}_{q,y_q}|\Psi\rangle\|^2$$
$$-\|M^{(i_1)}_{1,y_1}\cdots M^{(i_{q-1})}_{q-1,y_{q-1}}M^{(3)}_{l,y_l}\cdots M^{(3)}_{q+1,y_{q+1}}M^{(i_q)}_{q,y_q}|\Psi\rangle\|^2\big|$$
$$\le 2\sqrt{2\lambda_q},$$

or equivalently,

$$\sum_{y\in\{0,1\}^l}|p_{q-1}(y)-p_q(y)|\le 2\sqrt{2\lambda_q}.$$

Summing up this inequality for $1\le q\le l$, we obtain

$$\sum_{y\in\{0,1\}^l}|p_0(y)-p_l(y)|\le\sum_{q=1}^{l}2\sqrt{2\lambda_q}$$

by the triangle inequality, or equivalently,

$$\sum_{a_1,a_2,a_3\in\{0,1\}}\sum_{\substack{y\in\{0,1\}^l\\ y_{q_i}=a_i\ (i=1,2,3)}}|p_0(y)-p_l(y)|\le\sum_{q=1}^{l}2\sqrt{2\lambda_q}.$$

The claim follows by moving the summation over y inside the absolute value by using the triangle inequality. $\square$

Claim 2. *For distinct $q_1,q_2,q_3\in Q$,*

$$\sum_{a_1,a_2,a_3\in\{0,1\}}\big|P'(a_1a_2a_3\mid q_1q_2q_3)-P_{\mathrm{com}}(a_1a_2a_3\mid q_1q_2q_3)\big|$$
$$\le 2\sqrt{2\lambda_{q_1}}+2\sqrt{2\lambda_{q_2}}+2\sqrt{2\lambda_{q_3}}.$$

Proof. If $q_1<q_2<q_3$, sum up the two inequalities

$$\sum_{a_1,a_2,a_3\in\{0,1\}}\big|\|M^{(1)}_{q_1,a_1}M^{(1)}_{q_2,a_2}M^{(1)}_{q_3,a_3}|\Psi\rangle\|^2$$
$$-\|M^{(1)}_{q_1,a_1}M^{(1)}_{q_2,a_2}M^{(3)}_{q_3,a_3}|\Psi\rangle\|^2\big|\le 2\sqrt{2\lambda_{q_3}},$$
$$\sum_{a_1,a_2,a_3\in\{0,1\}}\big|\|M^{(3)}_{q_3,a_3}M^{(1)}_{q_1,a_1}M^{(1)}_{q_2,a_2}|\Psi\rangle\|^2$$
$$-\|M^{(3)}_{q_3,a_3}M^{(1)}_{q_1,a_1}M^{(2)}_{q_2,a_2}|\Psi\rangle\|^2\big|\le 2\sqrt{2\lambda_{q_2}},$$

each of which follows from Lemma 19, and use the triangle inequality. The other cases are proved similarly, where we use $P'(a_1a_2a_3\mid q_1q_2q_3)=\|M^{(i)}_{q_1,a_1}M^{(i)}_{q_2,a_2}M^{(i)}_{q_3,a_3}|\Psi\rangle\|^2$ with i such that q_i is the smallest in q_1,q_2,q_3. $\square$

197

By Claims 1 and 2, for any distinct $q_1, q_2, q_3 \in Q$,

$$\sum_{a_1, a_2, a_3 \in \{0,1\}} \big| P_{\mathrm{c}}(a_1 a_2 a_3 \mid q_1 q_2 q_3)$$
$$- P_{\mathrm{com}}(a_1 a_2 a_3 \mid q_1 q_2 q_3) \big|$$
$$\leq 2\sqrt{2\lambda_{q_1}} + 2\sqrt{2\lambda_{q_2}} + 2\sqrt{2\lambda_{q_3}} + \sum_{q=1}^{\max\{q_1, q_2, q_3\}} 2\sqrt{2\lambda_q}$$
$$\leq 4\sqrt{2} \sum_{q \in Q} \sqrt{\lambda_q}.$$

Therefore,

$$|w_{\mathrm{sim}} - s| \leq 4\sqrt{2} \sum_{q \in Q} \sqrt{\lambda_q} \leq 4\sqrt{2} \sqrt{|Q| \sum_{q \in Q} \lambda_q}$$
$$\leq 4\sqrt{2} \sqrt{2 \cdot 2^r |Q|(1 - w_{\mathrm{cons}})} \leq 8\sqrt{3} \cdot 2^r \sqrt{1 - w_{\mathrm{cons}}},$$

where the third inequality follows from the inequality (4) and the last inequality follows from the fact $|Q| \leq 3 \cdot 2^r$. This implies

$$8\sqrt{6} \cdot 2^r \sqrt{1 - w} = 8\sqrt{3} \cdot 2^r \sqrt{(1 - w_{\mathrm{sim}}) + (1 - w_{\mathrm{cons}})}$$
$$\geq 1 - w_{\mathrm{sim}} + 8\sqrt{3} \cdot 2^r \sqrt{1 - w_{\mathrm{cons}}} \geq 1 - s,$$

or equivalently $1 - w \geq (1/384)(1 - s)^2 \cdot 2^{-2r}$.

5.4. The two-prover case

Finally, the result by Cleve, Høyer, Toner and Watrous [6] essentially implies that it is efficiently decidable whether the entangled value of a given two-player one-round binary-answer game is equal to one or not. This proves Theorem 7.

Proof of Theorem 7. (i) For a two-player one-round binary-answer game G, $w_{\mathrm{q}}(G) = 1$ if and only if $w_{\mathrm{c}}(G) = 1$ [6, Theorem 5.12]. Therefore, the problem of deciding whether $w_{\mathrm{q}}(G) = 1$ or not is equivalent to a problem of deciding whether $w_{\mathrm{c}}(G) = 1$ or not. Since G is two-player and binary-answer, testing whether $w_{\mathrm{c}}(G) = 1$ or not can be cast as an instance of the 2SAT problem, and it is solvable in time polynomial in the number of questions.

(ii) This part follows from (i) since any classical two-prover one-round binary interactive proof system with entangled provers involves at most exponentially many questions. □

Acknowledgement

References

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

[2] J. Barrett and S. Pironio. Popescu–Rohrlich correlations as a unit of nonlocality. *Physical Review Letters*, 95(140401), 2005.

[3] 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*, pages 113–131, 1988.

[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[5] R. Cleve, D. Gavinsky, and R. Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive private information retrieval systems. arXiv:0707.1729v1 [quant-ph], 2007.

[6] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the Nineteenth IEEE Annual Conference on Computational Complexity*, pages 236–249, 2004.

[7] D.-Z. Du and K.-I. Ko. *Theory of Computational Complexity*. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 2000.

[8] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, pages 733–744, 1992.

[9] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134(2):545–557, 1994.

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

[11] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. arXiv:0704.2903v2 [quant-ph], 2007.

[12] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[13] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2001.

[14] A. Peres. *Quantum Theory: Concepts and Methods*, volume 57 of *Fundamental Theories of Physics*. Kluwer Academic Publishers, 1993.

[15] X. Sun, A. C.-C. Yao, and D. Preda. On entangled quantum 3-prover systems for SAT and the magic square. Invited talk at QIP 2007 presented by A. Yao, 2007.

[16] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[17] B. S. Tsirelson. Bell inequalities and operator algebras (Problem 33). In *Quantum Information: Open Problems*. 2006. http://www.imaph.tu-bs.de/qi/problems/33.html.

[18] S. Wehner. Tsirelson bounds for generalized Clauser–Horne–Shimony–Holt inequalities. *Physical Review A*, 73(022110), 2006.