Consequences and Limits of Nonlocal Strategies

Richard Cleve* Peter Høyer* Benjamin Toner† John Watrous*

Abstract

This paper investigates various aspects of the nonlocal effects that can arise when entangled quantum information is shared between two parties. A natural framework for studying nonlocality is that of cooperative games with incomplete information, where two cooperating players may share entanglement. Here nonlocality can be quantified in terms of the values of such games. We review some examples of nonlocality and show that it can profoundly affect the soundness of two-prover interactive proof systems. We then establish limits on nonlocal behavior by upper-bounding the values of several of these games. These upper bounds can be regarded as generalizations of the so-called Tsirelson inequality. We also investigate the amount of entanglement required by optimal and nearly optimal quantum strategies.

1. Introduction

In this paper, we develop methods for establishing limits on the kinds of nonlocal strategies that are possible with quantum entanglement. For example, we obtain some new *Tsirelson-type* inequalities, that bound the amount by which entanglement can be used to violate Bell-type inequalities.

Nonlocality can be naturally expressed within the framework of cooperative games of incomplete information—which we will refer to as *nonlocal games*. In this framework, there are two cooperating players and a verifier. The verifier sends a classical message to each player separately. Then each player, without communicating with the other, sends a classical response to the verifier, who evaluates a predicate to determine whether the players won or not. The players may share *a priori* information, but cannot communicate with each other once the game starts. In a *classical strategy*, the players can only share classical information; whereas, in a *quantum strategy*, the players are permitted to share quantum information. The *value* of such a game is the maximum possible success probability of the players. Bell inequalities can be expressed as upper bounds on the values of these games when the players are restricted to classical strategies. Bell inequality violations correspond to quantum strategies that exceed the classical value of games. Tsirelson inequalities are upper bounds on the values of these games when the players may employ quantum strategies.

One motive for investigating this subject is to better understand the expressive power of two-prover interactive proof systems when the provers share entanglement, which correspond closely to these games when the interaction is restricted to one round. One striking observation is that entanglement can affect the soundness of these proof systems. Based on Bell inequality violations, we give examples of such proof systems that are classically sound, but become unsound when the provers can utilize entanglement. One motive for investigating Tsirelson inequalities is that they arise as necessary conditions for the soundness of such proof systems when the provers share entanglement.

In Section 2 we provide some formal definitions and background information. In Section 3 we present four examples of nonlocal games for which quantum strategies outperform classical strategies, including nonlocal games for which there exist perfect quantum strategies (meaning that the strategies win with probability one), but for which there do not exist perfect classical strategies. The examples are not new, but for the most part have been presented in the theoretical physics literature as hypothetical physics experiments, and their connections with our games or with multi-prover interactive proofs are obscure. The simplicity of some of our presentations (particularly our fourth example) may help elucidate some of the features of nonlocality. In Section 4, we exhibit two natural two-prover interactive proof systems that are classically sound but become unsound when the provers may employ quantum strategies. In Section 5, we provide the beginnings of a systematic understanding of the limits of nonlocal strategies for two restricted classes of games: *binary games* and *XOR games*. The results proved in this section include generalizations of Tsirelson's inequality. We also prove upper bounds on the amount of entanglement needed to play XOR games optimally or nearly optimally.

* Institute for Quantum Information Science and Department of Computer Science, University of Calgary, Calgary, Alberta, Canada. Email: {cleve, hoyer, jwatrous}@cpsc.ucalgary.ca

† Institute for Quantum Information and Department of Physics, California Institute of Technology, Pasadena, California, USA. Email: toner@theory.caltech.edu

Proceedings of the 19th IEEE Annual Conference on Computational Complexity (CCC'04)
1093-0159/04 $20.00 © 2004 **IEEE**

2. Definitions

Nonlocal games

Let V be a predicate on $S \times T \times A \times B$, for finite sets S, T, A, and B, and let π a probability distribution on $S \times T$. Then V and π define a *nonlocal* game $G(V, \pi)$ as follows. A pair of questions $(s, t) \in S \times T$ is randomly chosen according to the distribution π, and s is sent to player 1 and t is sent to player 2. Hereafter we will refer to player 1 as Alice and player 2 as Bob. Alice must respond with an answer $a \in A$ and Bob with an answer $b \in B$. Alice and Bob are not permitted to communicate after receiving s and t, but they may agree on whatever sort of strategy they like prior to receiving their questions. They win if V evaluates to 1 on (s, t, a, b) and lose otherwise. To stess the fact that (a, b) is correct or incorrect given questions (s, t) we will denote the value of the predicate V on (s, t, a, b) as $V(a, b \,|\, s, t)$.

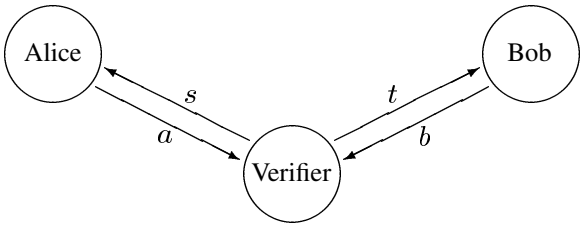

Figure 1. The communication structure of a nonlocal game.

Classical values of nonlocal games

The *classical value* of a game $G(V, \pi)$ is the maximum probability with which Alice and Bob can win the game, assuming they use purely classical strategies. Denote the classical value of a game $G = G(V, \pi)$ by $\omega_c(G)$. A *deterministic* strategy, is a restricted type of classical strategy in which a and b are simply functions of s and t, respectively. It is not hard to see that the classical value of a game is obtained on some deterministic strategy, and thus

$$\omega_c(G(V, \pi)) = \max_{a,b} \sum_{s,t} \pi(s, t) V(a(s), b(t) \,|\, s, t).$$

Quantum strategies and quantum values of games

We will assume for this discussion and throughout the rest of the paper that the reader is familiar with the basics of quantum information, which is discussed in detail in the book by Nielsen and Chuang [35].

A quantum strategy for a game G consists of an initial bipartite state $|\psi\rangle$ shared by Alice and Bob, a quantum measurement for Alice for each $s \in S$, and a quantum measurement for Bob for each $t \in T$. On input (s, t), Alice performs her measurement corresponding to s on her portion of $|\psi\rangle$, yielding an outcome a. Similarly, Bob performs his measurement corresponding to t on his portion of $|\psi\rangle$, yielding outcome b. The results a and b are sent back to the verifier.

The most general type of measurement allowed by quantum physics is called a positive operator valued measure, or POVM for short. Any such measurement of a system having classical state set Σ can be described by some collection of positive semidefinite matrices $\{X^a : a \in A\}$ in $\mathbb{C}^{\Sigma \times \Sigma}$, where A is a finite set that corresponds to the possible outcomes of the measurement. These matrices must satisfy $\sum_{a \in A} X^a = I$ (the identity operator on $\mathbb{C}^{\Sigma}$). If the measurement described by $\{X^a : a \in A\}$ is applied to a system in state $|\psi\rangle$, the outcome is a with probability $\langle\psi|X^a|\psi\rangle$ for each $a \in A$. These probabilities are all non-negative because each X^a is positive semidefinite, and the probabilities sum to 1 because $\sum_{a \in A} X^a = I$.

With the definition of POVMs in mind, a more precise description of a quantum strategy may be given as follows. Alice and Bob share some bipartite quantum state $|\psi\rangle \in \mathbb{C}^{\Sigma \times \Gamma}$. For each $s \in S$, Alice has a POVM described by

$$\{X_s^a : a \in A\} \subseteq \mathbb{C}^{\Sigma \times \Sigma},$$

and for each $t \in T$, Bob has a POVM described by

$$\{Y_t^b : b \in B\} \subseteq \mathbb{C}^{\Gamma \times \Gamma}.$$

On input $(s, t) \in S \times T$, Alice applies her POVM corresponding to s to the portion of $|\psi\rangle$ in her possession and Bob does likewise. Then Alice and Bob each return the result of their measurement to the verifier. The probability that Alice and Bob answer $(a, b) \in A \times B$ is given by

$$\langle\psi|X_s^a \otimes Y_t^b|\psi\rangle,$$

where $\otimes$ denotes the Kronecker product.

The *quantum value* of a game $G(V, \pi)$, denoted $\omega_q(G)$, is the maximum probability with which Alice and Bob can win over all possible quantum strategies.

3. Examples of nonlocal games

The fact that entanglement can cause non-classical correlations is a familiar idea in quantum physics, introduced in a seminal 1964 paper by Bell [5]. In the following subsections, we give four examples of this. The first is a slight variant of Bell's original result, which is simple and included as an introduction. The remaining ones can be viewed as generalizations or improvements, in various respects, to the first one.

3.1. The CHSH game

Our first example of a game for which a quantum strategy outperforms any classical strategy is a well-known example in quantum physics based on the CHSH inequality, named for its discoverers Clauser, Horne, Shimony, and Holt [13]. Rephrased in terms of two-player cooperative games, the example is as follows. Let $S = T = A = B = \{0,1\}$, let π be the uniform distribution on $S \times T$, and let V be the predicate

$$V(a,b \,|\, s,t) = \begin{cases} 1 & \text{if } a \oplus b = s \wedge t \\ 0 & \text{otherwise.} \end{cases}$$

The classical value of the game $G = G(V,\pi)$ is $\omega_c(G) = 3/4$, which is easily verified by considering all deterministic strategies. Using a quantum strategy, however, Alice and Bob can win this game with probability $\cos^2(\pi/8) \approx 0.85$, and this quantum strategy is optimal, so we have $\omega_q(G) = \cos^2(\pi/8)$. We next describe a quantum strategy that achieves this probability of success; the fact that it is optimal follows from Tsirelson's Inequality [28, 39].

First, let the entangled state shared by Alice and Bob be $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Then, define

$$|\phi_0(\theta)\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle,$$
$$|\phi_1(\theta)\rangle = -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle,$$

and let Alice and Bob's measurements be given as

$$X_0^a = |\phi_a(0)\rangle\langle\phi_a(0)|,$$
$$X_1^a = |\phi_a(\pi/4)\rangle\langle\phi_a(\pi/4)|,$$
$$Y_0^b = |\phi_b(\pi/8)\rangle\langle\phi_b(\pi/8)|,$$
$$Y_1^b = |\phi_b(-\pi/8)\rangle\langle\phi_b(-\pi/8)|$$

for $a, b \in \{0,1\}$. It is now clear that each matrix is positive semidefinite. (Each matrix is actually a projection, so the measurements Alice and Bob are making are examples of projective measurements.) Given our particular choice of $|\psi\rangle$, we have $\langle\psi|X \otimes Y|\psi\rangle = \frac{1}{2}\operatorname{tr} X^{\mathsf{T}}Y$ for arbitrary X and Y. Thus, as each of the matrices X_s^a and Y_t^b is real and symmetric, the probability that Alice and Bob answer (s,t) with (a,b) is $\frac{1}{2}\operatorname{tr} X_s^a Y_t^b$. It is now routine to check that in every case, the correct answer is given with probability $\cos^2(\pi/8)$ and the incorrect answer with probability $\sin^2(\pi/8)$.

3.2. The Odd Cycle game

For the following game, imagine that Alice and Bob are trying to convince the verifier that an odd cycle of length n is 2-colorable (which it is not, as n is odd). The verifier sends the name of a vertex to each of Alice and Bob such that the two vertices are either the same or adjacent. Alice and Bob each send one of two colors back to the verifier. The verifier's requirement is that, when the vertices are the same, the two colors should agree, and when the vertices are adjacent, the colors should be different.

Formally, let $n \geq 3$ be an odd integer, $S = T = \mathbb{Z}_n$ and $A = B = \{0,1\}$. Let π be uniform over the set $\{(s,t) \in \mathbb{Z}_n \times \mathbb{Z}_n : s = t \text{ or } s+1 \equiv t \,(\mathrm{mod}\, n)\}$ and let V be defined as

$$V(a,b \,|\, s,t) = \begin{cases} 1 & \text{if } a \oplus b = [s+1 \equiv t \,(\mathrm{mod}\, n)] \\ 0 & \text{otherwise.} \end{cases}$$

This is a variation on a game based on the Chained Bell Inequalities of Braunstein and Caves [10] that generalize the CHSH inequality. It is also discussed by Vaidman [41].

It is easy to see that $\omega_c(G) = 1 - 1/2n$ for this game. Any deterministic strategy must fail for at least one of the possible pairs (s,t), as an odd cycle cannot be 2-colored, while a strategy achieving success probability $1 - 1/2n$ is that Alice and Bob let $a = s \bmod 2$ and $b = t \bmod 2$.

On the other hand, a quantum strategy can attain a success probability quadratically closer to 1. The following quantum strategy [10] wins with probability

$$\cos^2(\pi/4n) \geq 1 - (\pi/4n)^2.$$

The entanglement is a single EPR pair

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Define

$$\alpha_s = \left(\frac{\pi}{2} - \frac{\pi}{2n}\right)s + \frac{\pi}{4n},$$
$$\beta_t = \left(\frac{\pi}{2} - \frac{\pi}{2n}\right)t,$$
$$X_s^a = |\phi_a(\alpha_s)\rangle\langle\phi_a(\alpha_s)|,$$
$$Y_t^b = |\phi_b(\beta_t)\rangle\langle\phi_b(\beta_t)|,$$

where $|\phi_0(\theta)\rangle$ and $|\phi_1(\theta)\rangle$ are as defined in the previous section. Given questions (s,t), the probability that Alice and Bob answer the same bit may be calculated to be $\cos^2(\alpha_s - \beta_t)$, which implies they answer different bits with probability $\sin^2(\alpha_s - \beta_t)$. In case $s = t$ we have $\alpha_s - \beta_t = \pi/4n$, so they answer correctly (i.e., with $a = b$) with probability $\cos^2(\pi/4n)$, and in case $s+1 \equiv t \pmod{n}$ we have $\alpha_s - \beta_t = \pi/2 - \pi/4n$, so they answer correctly (i.e., with $a \neq b$) with probability $\sin^2(\pi/2 - \pi/4n) = \cos^2(\pi/4n)$. Therefore this strategy answers correctly with probability $\cos^2(\pi/4n)$ on every pair of questions. In fact this quantum strategy is optimal, as we shall show in Corollary 5.11 below.

3.3. The Magic Square game

The next game we consider is based on the fact that there does not exist a 3×3 binary matrix with the property that

each row has even parity and each column has odd parity. It is a slight variation of an example presented by Aravind [3], which builds on work by Mermin [33, 34]. The idea is to ask Alice to fill in the values in either a row or a column of the matrix (randomly selected) and to ask Bob to fill in a single entry of the matrix, that is randomly chosen among the three entries given to Alice. The requirement is that the parity conditions are met by Alice's answers (even for rows, odd for columns) and that Bob's answer is consistent with Alice's answers.

Formally, let $S = \mathbb{Z}_6$ index the six possible queries to Alice (three rows plus three columns) and let $T = \mathbb{Z}_9$ index the nine possible queries to Bob (one for each entry of the matrix). Let $A = \{0,1\}^3$ and $B = \{0,1\}$. The predicate $V(a,b\,|\,s,t)$ is defined to take value 1 if and only if a has the appropriate parity (0 for a row and 1 for a column) and the entry of a corresponding to t has value b. The distribution π is the uniform distribution over $\{(s,t) \in S \times T$: entry t is in triple $s\}$. It is not hard to see that $\omega_c(G) = 17/18$ for this game. It should be noted that, although it is convenient to set $A = \{0,1\}^3$ for this game, we could take $A = \{0,1\}^2$, because the third bit of Alice's output is determined by the first two bits and the parity constraints.

Remarkably, $\omega_q(G) = 1$ for this game—there exists a quantum strategy for Alice and Bob that wins every time. The essential ideas for such a strategy are discussed in [3] (where a slight variant of this game is presented).

3.4. The Kochen-Specker game

This game is based on the Kochen-Specker Theorem, which can be stated as follows.

Theorem 3.1 (Kochen and Specker [30]). *There exists an explicit set of vectors $\{v_0, \ldots, v_{m-1}\}$ in $\mathbb{R}^3$ that cannot be $\{0,1\}$-colored so that both of the following conditions hold:*
1. For every orthogonal pair of vectors v_i and v_j, they are not both colored 1.
2. For every mutually orthogonal triple of vectors v_i, v_j, and v_k, at least one of them is colored 1.

The original theorem in [30] used 117 vectors, but this has subsequently been reduced to 31 vectors [36]. We will assume that every orthogonal pair of vectors in the set is part of an orthogonal triple—which is easily achieved by adding a few more vectors to the set—and that the vectors are normalized. Connections between the Kochen-Specker Theorem and nonlocality have previously been made in [26].

The Kochen-Specker game is defined relative to the above set of vectors. Alice receives a random triple of orthogonal vectors as her input and Bob receives a single vector randomly chosen from the triple as his input. Alice outputs a trit indicating which of her three vectors is assigned color 1 (implicitly, the other two vectors are assigned color 0). Bob outputs a bit assigning a color to his vector. The requirement is that Alice and Bob assign the same color to the vector that they receive in common.

It is straightforward to show that the existence of a perfect classical strategy for this game would violate the Kochen-Specker Theorem, so $\omega_c(G) < 1$ for this game. On the other hand there is a perfect quantum strategy, using entanglement $|\psi\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$. Alice's projectors (for input v_i, v_j, v_k) are $|v_i\rangle\langle v_i|$, $|v_j\rangle\langle v_j|$, $|v_k\rangle\langle v_k|$, and Bob's projectors (for input v_l) are $|v_l\rangle\langle v_l|$ and $I - |v_l\rangle\langle v_l|$.

4. Connections with multi-prover interactive proof systems

The two-prover interactive proof system model was defined by Ben-Or, Goldwasser, Kilian, and Wigderson [7], and has been the focus of a great deal of study. Babai, Fortnow, and Lund [4] proved that every language in NEXP has a two-prover interactive proof system. Several refinements to this result were made [12, 16, 32], leading to a proof by Feige and Lovász [17] that a language is in NEXP if and only if it has a two-prover one-round proof system with perfect completeness and exponentially small soundness error.

In essentially all work on multi-prover interactive proof systems, the provers are computationally unbounded, subject to the restriction that they cannot communicate with each other during the course of the protocol. Because the spirit of the interactive proof system paradigm is to bound the capabilities of the verifier rather than the prover(s), it is natural to consider prover strategies that entail sharing entangled quantum information prior to the execution of the proof system. Note that such a strategy does not necessarily require the computationally bounded verifier to manipulate (or know anything about) quantum information. However, much of the study of multi-prover interactive proof systems occurred prior to the mid 1990s, when quantum information was not well-known within the theoretical computer science community, and quantum strategies were generally not considered. In fact, the methodologies for analyzing these proof systems usually make the implicit assumption that provers are restricted to classical strategies.

In this section, we consider what happens when the provers can employ quantum strategies. We do not make any change to the verifier, who remains classical, and all communication between the verifier and the provers remains classical.[1] A natural question is: What is the expressive power of such proof systems?

1 Kobayashi and Matsumoto [29] consider a related but different model, where the provers *and* the verifier manipulate quantum information and quantum communication occurs between the verifier and the provers.

Let us use MIP and MIP* to distinguish between the cases of no shared entanglement and shared entanglement, respectively. That is, MIP denotes the class of languages recognized by multi-prover interactive proof systems where all communication between the provers and verifier is classical and the provers do not share entanglement (as has been implicitly assumed in previous contexts). The definition of MIP* is identical to that of MIP, except that the provers may share an arbitrary entangled quantum state at the beginning of the protocol. Furthermore, let MIP$[k]$ and MIP*$[k]$ denote the same classes, but with the number of provers fixed to k. It is known that MIP = MIP$[2]$ = NEXP. We do not know any relationships between MIP*, MIP*$[2]$ and NEXP, except the trivial containment MIP*$[2] \subseteq$ MIP*.

A *one-round* two-party interactive proof system is one where the interaction is restricted to two stages: a query stage where the verifier sends information to the provers, and a response stage where the provers send information to the verifier. Note that such a proof system associates a non-local game G_x to each string x with the following property. For all $x \in L$, the value of $\omega_q(G_x)$ is close to one, and, for all $x \notin L$, the value of $\omega_q(G_x)$ is close to zero.

We give two examples of natural two-prover one-round proof systems that are classically sound, but become unsound when the provers use quantum strategies: one is for languages that express graph chromatic numbers and the other is for 3-SAT. These examples are related to the examples in Section 2. We also explain why the existing proofs that equate MIP with NEXP break down in terms of their methodology in the case of MIP*. It is possible that MIP* = NEXP, but a different proof would be required for it. Results in [29] imply that, if the amount of entanglement between the provers is polynomially bounded, then any language recognized by such a proof system is contained in NEXP; however, without this polynomial restriction, we do not know if this holds.

4.1. Graph Coloring proof system

The Odd Cycle game in Section 3.2 can be regarded as a protocol where two provers are trying to convince a verifier that a particular graph is two-colorable. This idea generalizes to any graph G and number of colors k. The verifier asks each prover for the color (among k possibilities) of a vertex and requires that the colors be the same whenever each prover gets the same vertex and different whenever the provers get adjacent vertices. Formally, the game for G and k is as follows. Let $S = T = V(G)$, let $A = B = \mathbb{Z}_k$, let

$$V(a,b\,|\,s,t) = \begin{cases} 1 & \text{if } (s = t \text{ and } a = b) \text{ or} \\ & ((s,t) \in E(G) \text{ and } a \neq b) \\ 0 & \text{otherwise,} \end{cases}$$

and π be the uniform distribution on

$$\{(s,s) : s \in V(G)\} \cup \{(s,t) \in E(G)\}.$$

If G is k-colorable then the provers can satisfy V by basing their answers on a valid coloring of G. Therefore, the value of the associated game is 1. If G is not k-colorable then, for any classical strategy on the part of the provers, there must be an inconsistency for some value of (s,t), so the classical value of the associated game is at most $1 - 1/(|V(G)| + |E(G)|)$. The verifier can amplify the difference between the two cases (k-colorable and not k-colorable) by repeating this game a polynomial number of times (in parallel [37]). Thus this is a classical two-prover interactive proof system for the language consisting of all k-colorable graphs.

This proof system breaks down in the case of entangled provers. Based on a protocol in [9], there exists a sequence of graphs G_n (where n ranges over all powers of two) with the following properties. First, for any n, there is a *perfect* quantum strategy for the Graph Coloring proof system with graph G_n and $k = n$ colors. Second, for sufficiently large n, G_n is not n-colorable.

For any n, G_n is simple to describe: it has vertices $\{0,1\}^n$ and two vertices are adjacent if and only if the Hamming distance between them is $n/2$. However, results in [9] show that *there exists* an n such that G_n is not n-colorable, without giving an explicit n for which this holds. (The proof is based on a related result in [11], which makes use of a combinatorial result in [21].) The result is made explicit in [22], where it is shown that G_{16} is not 16-colorable. Thus, the resulting graph for which the Graph Coloring proof system breaks down has 2^{16} vertices, and it can be simplified by taking only half of its vertices, resulting in a graph of 32,768 vertices.

4.2. 3-SAT proof system

We begin by describing a commonly-used two-prover interactive proof system for proving that 3-CNF formulas are satisfiable. Call the provers Alice and Bob. The verifier sends Alice a clause and Bob a variable from that clause. Alice must assign each variable from the clause so as to satisfy the clause and Bob must assign a value for the variable that he receives that is consistent with Alice's assignment. More, formally, let f be a 3-CNF boolean formula over variables $x_0, \ldots, x_{n-1}$ with m clauses $c_0, \ldots, c_{m-1}$. For each clause, every $a \in \{0,1\}^3$ induces an assignment to each variable that occurs in the clause in a natural way. The game for f is as follows. Let $S = \mathbb{Z}_m$ and $T = \mathbb{Z}_n$, let $A = \{0,1\}^3$ and $B = \{0,1\}$, and let $V(a,b\,|\,s,t)$ take the value 1 if and only if the assignment for the variables in c_s induced by a satisfies c_s and is consistent with the assignment $x_t = b$. Let π be the uniform distribution on

$\{(s,t) \in S \times T :$ clause c_s contains variable $x_t\}$. If f is satisfiable then $\omega_c(f) = 1$ by the two provers returning values corresponding to a specific truth assignment. If f is unsatisfiable then $\omega_c(f) \leq 1 - 1/3m$, as then at least one of the $3m$ possible (s,t) queries must violate the predicate.

However, this proof system breaks down in the case of entangled provers. Upon seeing the aforementioned counterexample for the Graph Coloring proof system, Ambainis [2] showed that a counterexample for 3-SAT could be based on it. Intuitively, the idea is to construct a 3-CNF formula that, for truth assignment x, expresses the statement "x is a k-coloring of G". Based on the above counterexample graph with 32,768 vertices (the smallest that we are aware of), the resulting 3-SAT formula consists of roughly 10^8 clauses.

We now provide a much simpler counterexample based on the Magic Square game in Section 3.3 that consists of 24 clauses. We will construct an instance of 3-SAT, where the resulting formula is not satisfiable but for which there is a perfect quantum strategy for the above two-prover proof system. Let the variables be x_{00}, x_{01}, x_{02}, x_{10}, x_{11}, x_{12}, x_{20}, x_{21}, x_{22}, which intuitively correspond to a 3×3 boolean matrix. There are six parity conditions in the Magic Square game: each row has even parity and each column has odd parity. Each parity condition can be expressed with four clauses. For example, for the first row,

$$(\overline{x}_{00} \vee \overline{x}_{01} \vee \overline{x}_{02}) \wedge (\overline{x}_{00} \vee x_{01} \vee x_{02}) \\ \wedge (x_{00} \vee \overline{x}_{01} \vee x_{02}) \wedge (x_{00} \vee x_{01} \vee \overline{x}_{02})$$

is satisfied if and only if $x_{00} \oplus x_{01} \oplus x_{02} = 0$. Thus 24 clauses suffice to express all six parity conditions. This formula is unsatisfiable, but the perfect quantum strategy for the Magic Square game in Section 3.3 defeats the 3-SAT game for this formula with certainty.

4.3. Oracularization paradigm

The above example also constitutes a counterexample to a commonly-used primitive that enables a two-prover system to simulate an *oracle machine*. An oracle machine is a one-prover interactive system where the prover's responses to a series of questions are required to be *non-adaptive*. Non-adaptive means that when the prover receives a series of queries $s_1, s_2, \ldots, s_m$, his response to s_i must be a function of s_i alone, not depending on any s_j for $j \neq i$. There is a simple oracle machine proof system for 3-SAT, where a random clause is selected and its three variables are sent as three queries to the prover, who must return a value for each one. The verifier accepts if and only if the responses satisfy the clause. The prover's success probability is less than one whenever the formula is unsatisfiable.

Fortnow, Rompel, and Sipser [20] showed that, with a second prover, who is sent a single randomly chosen query from those of the first prover, the first prover must behave as an oracle or be detected with positive probability. Nevertheless, the above quantum strategy for the magic square game is a counterexample to this result for the case of entangled provers. Since this is a component in the proof that MIP = NEXP, this proof does not carry over to the case of MIP*.

5. Binary games and XOR games

In this section we focus our attention on simple types of games that we call *binary games* and *XOR games*. Binary games are games in which Alice and Bob's answers are bits: $A = B = \{0,1\}$. XOR games are binary games that are further restricted in that the value of the predicate V may depend only on $a \oplus b$ and not on a and b independently. (The CHSH and Odd Cycle games are examples of XOR games.)

We begin by pointing out connections between these games and multi-prover interactive proof systems. Then we establish some basic properties of binary games and XOR games. Next, we prove upper bounds on the quantum values of these games. Finally, we prove upper bounds on the amount of entanglement required for Alice and Bob to play XOR games optimally and nearly optimally.

5.1. Further connections with multi-prover interactive proof systems

One motive for considering upper bounds on the quantum values of games in general is due to their connections with multi-prover interactive proof systems. For example, recall that the Odd Cycle game can be regarded as a simple proof system for the two-colorability of odd cycles—for which the correct response of the verifier is to reject. Although this is valid as a classical two-prover interactive proof system, if the quantum value of the game were one (or exponentially close to one) then it would not be valid as a quantum proof system. The upper bound on the value of the Odd Cycle game proved in this section (Corollary 5.11) implies that it is a valid quantum proof system, and with a polynomial number of repetitions[2], the probability of the verifier incorrectly accepting can be made arbitrarily close to zero. For any one-round two-prover quantum interactive proof system, the soundness condition will correspond to a nontrivial upper bound of the quantum value of a nonlocality game. Therefore upper bounds are important tools for analyzing such proof systems.

Regarding upper bounds on entanglement required by an optimal quantum strategy, we note that results in [29] imply that if a polynomial upper bound can be established then

2 In the absence of a quantum analogue of Raz's Parallel Repetition Theorem [37], the repetitions can be applied sequentially.

$\mathrm{MIP}^*[2] \subseteq \mathrm{NEXP}$. This indicates that upper bounds on entanglement are also relevant for analyzing such proof systems.

Definition 5.1. For $0 \leq s < c \leq 1$, let $\oplus\mathrm{MIP}_{c,s}[2]$ denote the class of all languages L recognized by classical two-prover interactive proof systems 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 Alice and Bob follow, the Prover's acceptance probability is at most s (the *soundness* probability).
- If $x \in L$ then there exists a strategy for Alice and Bob for which the Prover's acceptance probability is at least c (the *completeness* probability).

Definition 5.2. For $0 \leq s < c \leq 1$, let $\oplus\mathrm{MIP}^*_{c,s}[2]$ denote the class corresponding to the previous definition, where all communication remains classical, but where the provers may share prior quantum entanglement.

The following result is implicit in the work of Håstad [25], with the application of methods in [6].

Theorem 5.3. *For all $\varepsilon \in (0, 1/16)$, if $s = 11/16 + \varepsilon$ and $c = 12/16$ then $\oplus\mathrm{MIP}_{c,s}[2] = \mathrm{NEXP}$.*

Proof sketch. We refer the reader to [6, 25] for all detailed information about probabilistically checkable proof systems (PCPs). Let $\mathrm{PCP}_{c,s}[r,k]$ denote the class of languages recognized by PCPs that makes k queries on the basis of r random bits, and have completeness and soundness probabilities c and s respectively. That is, a verifier can query k bits of a purported proof, selected on the basis of r random bits, and makes a determination of language membership on the basis of those k values. A language L is in $\mathrm{PCP}_{c,s}[r,k]$ if: (a) for all $x \in L$, there exists a proof for which the verifier's acceptance probability is at least c; and (b) for all $x \notin L$, the verifier's acceptance never exceeds s. Håstad [25] essentially shows that, for all $\varepsilon > 0$, if $s = 11/16 + \varepsilon$, and $c = 12/16$ then $\mathrm{PCP}_{c,s}[O(\log n), 2] = \mathrm{NP}$ using PCPs where the verifier's determination is based on the XOR of the two queried bits. This can be scaled up one exponential in n along the lines discussed in [6] to yield $\mathrm{PCP}_{c,s}[n^{O(1)}, 2] = \mathrm{NEXP}$ with the same XOR property. Moreover, the proof system has the feature that, if each possible pair of queries is taken as an edge of a graph then the resulting graph is bipartite. This means that the PCP can be converted into a two-prover interactive proof system with the same completeness and soundness probabilities (c and s) as follows. The verifier randomly chooses an edge, just as in the PCP, and sends one query to Alice and one to Bob, according to the bipartite structure of the graph. ■

An obvious question is: Do there exist c and s (with $0 \leq s < c \leq 1$) such that $\oplus\mathrm{MIP}^*_{c,s}[2] = \mathrm{NEXP}$? One natural candidate for this is the actual protocol implicit in [25]. Unfortunately, our generic upper bounds, such as Theorem 5.10, are not sufficiently strong to achieve this—at least not directly, since they result in a larger value of s, which exceeds the original c. Perhaps an analysis that is tailored to the specific constructions in [25] will show that the required c and s exist.

5.2. Basic properties of binary and XOR games

In this section it is proved that for any binary game, Alice and Bob always have an optimal strategy in which their measurements are projective measurements, even when restricted to the support of their respective parts of the shared entangled state. Alice and Bob's strategy for a binary game consists of a shared entangled state $|\psi\rangle \in \mathbb{C}^{\Sigma\times\Gamma}$, together with POVMs $\{X_s^0, X_s^1\} \subseteq \mathbb{C}^{\Sigma\times\Sigma}$ and $\{Y_t^0, Y_t^1\} \subseteq \mathbb{C}^{\Gamma\times\Gamma}$ for each $s \in S$ and $t \in T$, respectively. By the support of Alice's part of the entangled state, we mean the subspace of $\mathbb{C}^{\Sigma}$ spanned by the eigenvectors of the density matrix obtained by tracing out Bob's part of $|\psi\rangle$, and similar for the support of Bob's part. It follows from the Schmidt decomposition that these two subspaces will necessarily have the same dimension.

It is well known that POVM-type measurements can be simulated by projective measurements. In general this requires that one performs a projective measurement on the system under consideration together with some auxiliary system, and in the present situation this auxiliary system may be considered part of the shared entangled state. However, the fact we are claiming is a stronger statement than this—even if the measurements $\{X_s^0, X_s^1\} \subseteq \mathbb{C}^{\Sigma\times\Sigma}$ and $\{Y_t^0, Y_t^1\} \subseteq \mathbb{C}^{\Gamma\times\Gamma}$ describe projective measurements, they may no longer be projections when restricted to the support of Alice's part and of Bob's part of $|\psi\rangle$.

Theorem 5.4. *Let G be a binary game. Then there exists an optimal strategy for Alice and Bob that satisfies the following:*

1. *The entangled state shared by Alice and Bob is $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$, where $\dim(\mathcal{A}) = \dim(\mathcal{B})$ and both $\mathrm{tr}_{\mathcal{A}} |\psi\rangle\langle\psi|$ and $\mathrm{tr}_{\mathcal{B}} |\psi\rangle\langle\psi|$ are invertible. (I.e., $\mathcal{A}$ is the support of Alice's part of $|\psi\rangle$ and $\mathcal{B}$ is the support of Bob's part of $|\psi\rangle$.)*
2. *Alice's measurements $\{X_s^0, X_s^1\}$ and Bob's measurements $\{Y_t^0, Y_t^1\}$, for $s \in S$ and $t \in T$, are projective measurements on $\mathcal{A}$ and $\mathcal{B}$, respectively.*

The proof of Theorem 5.4 relies on the following simple lemma.

Lemma 5.5. *Let S, T, and B be finite sets and let $A = \{0,1\}$. Let $\{Z_t^b : t \in T, b \in B\}$ be Hermitian $N \times N$ matrices, let $\{\alpha_{s,t,a,b} : s \in S, t \in T, a \in A, b \in B\}$ be real numbers, and let X be an $N \times N$ positive semidefinite matrix. Then the maximum value of*

$$\sum_{s,t,a,b} \alpha_{s,t,a,b} \operatorname{tr}(X_s^a Z_t^b)$$

for $\{X_s^a : s \in S, a \in A\}$ positive semidefinite $N \times N$ matrices subject to the constraint $X_s^0 + X_s^1 = X$ for all $s \in S$ is achieved by some choice of $\{X_s^a\}$ for which $\operatorname{tr}(X_s^0 X_s^1) = 0$ for all $s \in S$.

Proof. The fact that there exists a maximum follows from the observation that the set of all valid choices for

$$\{X_s^a : s \in S, a \in A\}$$

is a compact set. Fix some choice for $\{X_s^a\}$ that achieves the maximum. Because each X_s^0 is positive semidefinite, we may write

$$X_s^0 = \sum_{j=1}^{N} \lambda_{s,j} |\psi_{s,j}\rangle\langle\psi_{s,j}|$$

for some orthonormal basis $\{|\psi_{s,1}\rangle, \ldots, |\psi_{s,N}\rangle\}$ for each $s \in S$. As X_s^0 and $X - X_s^0$ are both positive semidefinite, we have $0 \leq \lambda_{s,j} \leq c_{s,j} = \langle\psi_{s,j}|X|\psi_{s,j}\rangle$ for each s and j. Now, if we fix the bases $\{|\psi_{s,1}\rangle, \ldots, |\psi_{s,N}\rangle\}$ but view $\{\lambda_{s,j} : s \in S, 1 \leq j \leq N\}$ as being variables, we see that the quantity

$$\sum_{s,t,a,b} \alpha_{s,t,a,b} \operatorname{tr}(X_s^a Z_t^b)$$

is a multi-linear function in these variables. It therefore achieves its maximum value for some choice of these variables with $\lambda_{s,j} \in \{0, c_{s,j}\}$. For such a choice of these variables, the matrices X_s^0 and X_s^1 satisfy $\operatorname{tr}(X_s^0 X_s^1) = 0$ as required. ∎

Proof of Theorem 5.4. The fact that the first condition holds for some optimal strategy follows immediately from the Schmidt decomposition together with the fact that any POVM restricted to a subspace is still a valid POVM. So, we will assume that we have an optimal strategy satisfying the first condition, but not necessarily satisfying the second.

The probability that Alice and Bob's strategy wins is

$$\begin{aligned}
&\Pr[\text{Alice and Bob win}] \\
&\quad = \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b \,|\, s,t) \, \langle\psi| X_s^a \otimes Y_t^b |\psi\rangle \\
&\quad = \sum_{s,t,a,b} \pi(s,t) V(a,b \,|\, s,t) \, \operatorname{tr} X_s^a Z_t^b,
\end{aligned}$$

where

$$Z_t^b = \operatorname{tr}_{\mathcal{B}}(I \otimes Y_t^b)|\psi\rangle\langle\psi|$$

for each $t \in T$ and $b \in \{0,1\}$. It follows from Lemma 5.5 that Alice may substitute her measurements

$$\{X_s^a : s \in S, a \in \{0,1\}\}$$

with projective measurements on $\mathcal{A}$ while still achieving the maximum probability of winning. The same argument applies to Bob's measurements. ∎

We will make use of Theorem 5.4 several times below.

Next, we consider XOR games, which are binary games where the predicate $V(a,b \,|\, s,t)$ depends only on $c = a \oplus b$ and not a and b independently. It will be convenient to view the predicate V as taking only three inputs in this case—we write $V(a \oplus b \,|\, s,t)$ rather than $V(a,b \,|\, s,t)$. It will be particularly helpful for XOR games to describe Alice and Bob's measurements in terms of *observables*. Because of Theorem 5.4, it will only be necessary to do this in the case that Alice and Bob's measurements are projective measurements. If X^0 and X^1 are orthogonal projections with $X^0 + X^1 = I$, we can describe this measurement by an observable $X = X^0 - X^1$. It follows that the observable corresponding to a two-outcome projective measurement is a Hermitian matrix with eigenvalues $+1$ and -1, and the $+1$ eigenspace corresponds to the outcome 0 and the -1 eigenspace corresponds to the outcome $+1$.

The following theorem due to Tsirelson [40] will play a key role in our results on XOR games.

Theorem 5.6 (Tsirelson [40]). *Let S and T be finite sets, and let $|\psi\rangle$ be a pure quantum state with support on a bipartite Hilbert space $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ for which $\dim \mathcal{A} = \dim \mathcal{B} = n$. For each $s \in S$, let X_s be an observable on $\mathcal{A}$ with eigenvalues ± 1, and for each $t \in T$, let Y_t be an observable on $\mathcal{B}$ with eigenvalues ± 1. Then there exist real unit vectors x_s and y_t in $\mathbb{R}^{2n^2}$ such that*

$$\langle\psi| X_s \otimes Y_t |\psi\rangle = x_s \cdot y_t,$$

for all $s \in S$ and all $t \in T$.

Conversely, suppose that S and T are finite sets, and x_s and y_t are unit vectors in $\mathbb{R}^N$ for each $s \in S$ and $t \in T$. Let $\mathcal{A}$ and $\mathcal{B}$ be Hilbert spaces of dimension $2^{\lceil N/2 \rceil}$, let $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$, and let $|\psi\rangle$ be any maximally entangled state on $\mathcal{H}$. Then there exist observables X_s on $\mathcal{A}$ and Y_t on $\mathcal{B}$ with eigenvalues ± 1 such that

$$\langle\psi| X_s \otimes Y_t |\psi\rangle = x_s \cdot y_t,$$

for all $s \in S$ and all $t \in T$.

To state some upper bounds on $\omega_q(G)$ for XOR games, it will be helpful to define the *trivial random* strategy for Alice and Bob as one where they ignore their inputs and answer uniformly generated random bits. If $\tau(G)$ denotes the

success probability of game (G, π) when Alice and Bob are restricted to this trivial strategy, then

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

Proposition 5.7. *Let $G(V, \pi)$ be an XOR game and let $N = \min(|S|, |T|)$. Then*

$$\begin{aligned} &\omega_q(G) - \tau(G) \\ &= \frac{1}{2} \max_{x_s, y_t} \sum_{s,t} \pi(s,t) \left(V(0 \,|\, s,t) - V(1 \,|\, s,t) \right) x_s \cdot y_t, \end{aligned} \tag{1}$$

where the maximum is over unit vectors

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

Proof. By Theorem 5.4, it is sufficient to restrict to the case where Alice and Bob make projective measurements on the support of their component of a shared pure entangled state. Therefore, suppose that Alice and Bob share the entangled state $|\psi\rangle$ in some bipartite Hilbert space $\mathcal{A} \otimes \mathcal{B}$ with $\dim \mathcal{A} = \dim \mathcal{B} = n$. For each $s \in S$, let $X_s = X_s^0 - X_s^1$ be the observable corresponding to Alice's measurement on input s, and for each $t \in T$, let $Y_t = Y_t^0 - Y_t^1$ be the observable corresponding to Bob's measurement on input t. We now associate with each X_s a real unit vector x_s and with each Y_t a real unit vector y_t, according to Theorem 5.6. On input (s,t), the probability that $c = 0$ is

$$\begin{aligned} &\langle \psi | \left(X_s^0 Y_t^0 + X_s^1 Y_t^1 \right) | \psi \rangle \\ &\qquad = \frac{1}{2} \left(1 + \langle \psi | X_s \otimes Y_t | \psi \rangle \right) = \frac{1}{2} \left(1 + x_s \cdot y_t \right). \end{aligned}$$

It follows that $c = 1$ with probability $(1 - x_s \cdot y_t)/2$. Hence the probability that Alice and Bob win using this strategy is

$$\begin{aligned} &\frac{1}{2} \sum_{s,t,c} \pi(s,t) V(c \,|\, s,t) \\ &\qquad + \frac{1}{2} \sum_{s,t} \pi(s,t) \left(V(0 \,|\, s,t) - V(1 \,|\, s,t) \right) x_s \cdot y_t. \end{aligned}$$

The vectors x_s and y_t are unit vectors in $\mathbb{R}^{2n^2}$ where $n = \dim \mathcal{A} = \dim \mathcal{B}$ is *a priori* unbounded. The winning probability, however, depends only on the dot products of the unit vectors, so we may project onto the span of $\{x_s \,:\, s \in S\} \cup \{y_t \,:\, t \in T\}$. This space has dimension $M = |S| + |T|$. Indeed, it is sufficient to project the vectors $\{x_s \,:\, s \in S\}$ onto the span of the vectors $\{y_t \,:\, t \in T\}$ (or vice versa). The dimension of this space is at most $N = \min(|S|, |T|)$. Without loss of generality, let us assume $|S| \leq |T|$. Although the vectors $\{x_s \,:\, s \in S\}$ will not necessarily remain unit vectors after orthogonal projection, the maximum over all vectors $\{x_s \in \mathbb{R}^{|T|} \,:\, s \in S, \|x_s\| \leq 1\}$ is achieved by points on the boundary—unit vectors—and so it is sufficient to restrict to this case.

We now show this strategy can be realized as a quantum protocol. The maximization in Eq. 1 is over a compact set, so the maximum is achieved by some vectors $x_1, \ldots, x_{|S|}, y_1, \ldots, y_{|T|}$ in $\mathbb{R}^N$. Let $|\psi\rangle$ be a maximally entangled state on $\lceil N/2 \rceil$ qubits. By Theorem 5.6, there are observables $\{X_s\}$ and $\{Y_t\}$ such that

$$\langle \psi | X_s \otimes Y_t | \psi \rangle = x_s \cdot y_t$$

for all $s \in S$ and $t \in T$. Thus the strategy can be realized as a quantum protocol. ∎

The maximization in Proposition 5.7 can be cast as a semidefinite program, which can be approximated to within an additive error of ε in time polynomial in $|S| + |T|$ and in $\log(1/\varepsilon)$. (See Ref. [8] for an introduction to semidefinite programming.)

It is trivial to write an expression similar to Eq. 1 for the classical value of an XOR game, viz.,

$$\begin{aligned} &\omega_c(G) - \tau(G) \\ &= \frac{1}{2} \max_{a(s), b(t)} \sum_{s,t} \pi(s,t) (V(0 \,|\, s,t) - V(1 \,|\, s,t)) a(s) b(t), \end{aligned}$$

where the maximum is over functions $a : S \to \{-1, +1\}$ and $b : T \to \{-1, +1\}$. This integer quadratic program is MAXSNP hard [1]. Unless P = NP, finding the quantum value of an XOR game is easier than finding the classical value.

5.3. Upper bounds on values of binary and XOR games

In this section, we give some upper bounds on the quantum values of binary nonlocal games. We give two bounds for XOR games: the first is most useful when the optimal classical strategy is poor and the second when the optimal classical strategy is almost perfect. We also consider general binary games, where we obtain a qualitative upper bound for games with no perfect classical strategy.

5.3.1. Upper bound for XOR games with weak classical strategies We first consider the regime where the success probability of the best classical strategy is not much better than $\tau(G)$, the success probability of the trivial random strategy. In this case no quantum strategy can do significantly better. The bound will be expressed in terms of Grothendieck's constant [24].

Definition 5.8 ([18]). Grothendieck's constant K_G is the smallest number such that, for all integers $n \geq 2$ and all

$n \times n$ real matrices $H = (h_{st})$, if

$$\left| \sum_{s,t} h_{st}\, a_s b_t \right| \leq 1,$$

for all numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$ in $[-1, 1]$, then

$$\left| \sum_{s,t} h_{st}\, x_s \cdot y_t \right| \leq K_G,$$

for all unit vectors $x_1, \ldots, x_n, y_1, \ldots, y_n$ in $\mathbb{R}^n$.

Grothendieck's constant is known to satisfy

$$1.6769 \leq K_G \leq \frac{\pi}{2 \log\left(1 + \sqrt{2}\right)} \approx 1.7822,$$

but the exact value is not known. The upper bound is due to Krivine [31] (who conjectures it is the exact value), and the lower bound is due to Davie [15] and, independently, Reeds [38] (see also [19]).

The following theorem follows from the definition.

Theorem 5.9. *Let G be an XOR game. Then*

$$\omega_q(G) - \tau(G) \leq K_G \left[\omega_c(G) - \tau(G)\right].$$

Proof. Suppose, without loss of generality, that $|S| < |T|$. Let S' be the disjoint union of S and $\mathbb{Z}_{(|T|-|S|)}$ and define a game $G' = (V', \pi')$ on $S' \times T$ by setting $\pi'(s,t) = \pi(s,t)$ if $s \in S$ and $\pi'(s,t) = 0$ otherwise, and $V'(c\,|\,s,t) = V(c\,|\,s,t)$ for $s \in S$. Clearly this game is equivalent to the original game so it is sufficient to consider the case $|S| = |T|$.

Take $n = |S|$ and define the matrix H by

$$h_{st} = \frac{1}{2\left[\omega_c(G) - \tau(G)\right]} \pi(s,t) \left[V(0\,|\,s,t) - V(1\,|\,s,t)\right].$$

It follows from the discussion at the end of Section 5.2 that

$$\left| \sum_{s,t} h_{st}\, a_s b_t \right| \leq 1$$

for all numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$ in $[-1, 1]$. By Proposition 5.7,

$$\begin{aligned} \omega_q(G) - \tau(G) &= \left[\omega_c(G) - \tau(G)\right] \max_{x_s, y_s} h_{st}\, x_s \cdot y_s \\ &\leq K_G \left[\omega_c(G) - \tau(G)\right]. \end{aligned}$$

This establishes the result. ∎

For the CHSH game, we have $\tau(G) = 1/2$ and

$$\omega_q(G) - \tau(G) = \sqrt{2}\, \left[\omega_c(G) - \tau(G)\right].$$

Games for which the ratio of $\omega_q(G) - \tau(G)$ to $\omega_c(G) - \tau(G)$ is greater than $\sqrt{2}$ can be constructed from the results in Ref. [19]. In particular, the smallest known game for which this ratio is larger than $\sqrt{2}$ has $|S| = |T| = 20$.

5.3.2. Upper bound for XOR games with strong classical strategies We now consider the regime where a classical strategy performs well, but not perfectly. For the Odd Cycle game of Section 3.2, we obtained

$$\omega_c(G) = 1 - \frac{1}{2n}$$

and

$$\omega_q(G) \geq \cos^2(\pi/4n) \geq 1 - (\pi/4n)^2;$$

the quantum strategy is quadratically better than the classical one in terms of its failure probability. In fact such a quadratic improvement is all that is possible for XOR games, as will be shown shortly in Theorem 5.10.

In order to state and prove Theorem 5.10, we first define a function $g : [0,1] \to [0,1]$ and two constants, γ_1 and γ_2. The function g has the property that it is minimal subject to being concave and bounded below by $\sin^2(\frac{\pi}{2}x)$. To determine g, consider the unique linear mapping $h(x) = \gamma_1 x$ such that h is the tangent line to $\sin^2(\frac{\pi}{2}x)$ at some point $0 < \gamma_2 < 1$. It is straightforward to show that $g(x) = h(x)$ for $x \leq \gamma_2$ and $g(x) = \sin^2(\frac{\pi}{2}x)$ for $x > \gamma_2$. To determine the constants γ_1 and γ_2, note that the condition on h and the fact that $\frac{\mathrm{d}}{\mathrm{d}x} \sin^2(\frac{\pi}{2}x) = \frac{\pi}{2}\sin(\pi x)$ imply that

$$\frac{\pi}{2} \sin(\pi\gamma_2) \;=\; \frac{\sin^2(\frac{\pi}{2}\gamma_2)}{\gamma_2} \;=\; \gamma_1. \tag{2}$$

Theorem 5.10. *Let G be an XOR game with classical value $\omega_c(G)$. Then $\omega_q(G) \leq g(\omega_c(G))$, where g is as defined above, i.e.,*

$$\omega_q(G) \leq \begin{cases} \gamma_1 \omega_c(G) & \text{if } \omega_c(G) \leq \gamma_2 \\ \sin^2\left(\frac{\pi}{2}\omega_c(G)\right) & \text{if } \omega_c(G) > \gamma_2, \end{cases} \tag{3}$$

where $\gamma_1 \approx 1.1382$ and $\gamma_2 \approx 0.74202$ are as defined above.

Proof. Consider an optimal quantum strategy and let

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

be the unit vectors associated with it, according to Proposition 5.7. We use these vectors to define the following classical strategy:

1. Alice and Bob share a unit vector $\lambda \in \mathbb{R}^N$, chosen uniformly at random.
2. When asked question s, Alice answers
$$a' = \left[1 + \mathrm{sgn}(x_s \cdot \lambda)\right]/2.$$
3. When asked question t, Bob answers
$$b' = \left[1 + \mathrm{sgn}(y_t \cdot \lambda)\right]/2.$$

Here the sgn function is defined by $\mathrm{sgn}(x) = +1$ if $x \geq 0$ and -1 otherwise.

Let us calculate the probability that $a' \oplus b' = 1$. Introduce an azimuthal coordinate ϕ for λ in the plane spanned by x_s and y_t, such that x_s has coordinate $\phi = 0$ and y_t has coordinate $\phi = \theta_{st} \equiv \cos^{-1} x_s \cdot y_t \in [0, \pi]$. Then $\mathrm{sgn}(x_s \cdot \lambda) = 1$ for $\phi \in [-\pi/2, \pi/2]$ and -1 otherwise, while $\mathrm{sgn}(y_t \cdot \lambda) = 1$ for $\phi \in [\theta_{st} - \pi/2, \theta_{st} + \pi/2]$ and -1 otherwise. Because λ is distributed uniformly in $\mathbb{R}^N$, ϕ is distributed uniformly in $[0, 2\pi)$. The probability that $a \oplus b = 1$ is then proportional to the measure of the subset of $[0, 2\pi)$ on which $\mathrm{sgn}(x_s \cdot \lambda) = -\mathrm{sgn}(y_t \cdot \lambda)$. In particular, $a' \neq b'$ when

$$\phi \in [-\pi/2, \theta_{st} - \pi/2) \cup [\pi/2, \theta_{st} + \pi/2).$$

Therefore, on input (s, t),

$$\Pr[a' \oplus b' = 1] = \tfrac{1}{\pi}\,\theta_{st}. \tag{4}$$

Using the quantum strategy, the probability that $a \oplus b = 1$ is given by

$$\Pr[a \oplus b = 1] = \tfrac{1}{2}\,(1 - x_s \cdot y_t) = \sin^2\left(\tfrac{1}{2}\,\theta_{st}\right),$$

so that

$$\begin{aligned}&\Pr[a \oplus b = 1]\\ &\quad = \sin^2\left(\tfrac{\pi}{2}\Pr[a' \oplus b' = 1]\right) \leq g(\Pr[a' \oplus b' = 1]).\end{aligned}$$

Similarly, it can be shown that

$$\begin{aligned}&\Pr[a \oplus b = 0]\\ &\quad = \sin^2\left(\tfrac{\pi}{2}\Pr[a' \oplus b' = 0]\right) \leq g\left(\Pr[a' \oplus b' = 0]\right).\end{aligned}$$

For each $(s, t) \in S \times T$, let $\varpi_c(s, t)$ and $\varpi_q(s, t)$ be the probabilities of winning the game when using the classical and quantum strategies, respectively, given that question (s, t) was asked. From the above, together with the concavity of g, it follows that $\varpi_q(s, t) \leq g(\varpi_c(s, t))$. The overall probability of winning using the quantum strategy is

$$\begin{aligned}\sum_{s,t} \pi(s,t)\varpi_q(s,t) &\leq \sum_{s,t} \pi(s,t) g(\varpi_c(s,t))\\ &\leq g\left(\sum_{s,t} \pi(s,t)\varpi_c(s,t)\right)\\ &\leq g(\omega_c(G)),\end{aligned}$$

where we have again used the fact that g is concave. ∎

We emphasize that our means of defining the classical strategy in the above proof is not original; indeed we can trace the technique back to Grothendieck, who used it to establish the first upper bound on the constant that bears his name [24]. More recently, Goemans and Williamson used the same idea to derive randomized approximation algorithms for MAX CUT and related problems [23].

One consequence of Theorem 5.10 is that the quantum strategy for the Odd Cycle game given in Section 3.2 is optimal.

Corollary 5.11. *If G is the Odd Cycle game then $\omega_q(G) \leq \cos^2(\pi/4n)$.*

5.3.3. Upper bound for general binary games Finally, we prove the following qualitative Tsirelson-type bound on any binary game: if $\omega_c(G) < 1$ then $\omega_q(G) < 1$ as well. This result relies on the assumption that the game is binary—for example, the Kochen-Specker game discussed in Section 2 is a ternary-binary game (i.e., $A = \{0, 1, 2\}$ and $B = \{0, 1\}$) for which there exists a perfect quantum strategy but no perfect classical strategy.

Theorem 5.12. *Let G be a binary game. Then $\omega_c(G) = 1$ if and only if $\omega_q(G) = 1$.*

Proof. Because $\omega_q(G) \geq \omega_c(G)$ for any game G, it suffices to show that $\omega_q(G) = 1$ implies $\omega_c(G) = 1$.

Let us first assume that there exists a Hilbert space $\mathcal{A}$ and two collections of subspaces

$$\{V_s^a \,:\, s \in S, a \in \{0,1\}\} \text{ and } \{W_t^b \,:\, t \in T, b \in \{0,1\}\}$$

of $\mathcal{A}$ that satisfy the following properties:

1. $(V_s^0)^\perp = V_s^1$ and $(W_t^0)^\perp = W_t^1$ for each $s \in S$ and $t \in T$.
2. For every $(s, t) \in S \times T$ with $\pi(s, t) > 0$ and $a, b \in \{0, 1\}$ with $V(a, b \,|\, s, t) = 0$, we have $V_s^a \perp W_t^b$.

We will show that this assumption implies that there exists a perfect classical strategy for G. After this it will be shown that a perfect quantum strategy for G implies the existence of such a collection of subspaces.

For any 4-tuple (s, t, a, b) satisfying $\pi(s, t) > 0$ and $V(a, b \,|\, s, t) = 0$ we may conclude from the two properties above that $V_s^a \subseteq (W_t^b)^\perp = W_t^{\neg b}$ and $W_t^b \subseteq (V_s^a)^\perp = V_s^{\neg a}$. These relations induce a partial order on the collection of subspaces $\{V_s^a\} \cup \{W_t^b\}$. In order to distinguish this partial order from any incidental set relations that may hold among the subspaces $\{V_s^a\} \cup \{W_t^b\}$, we will use the symbol $\leq$ when referring to this partial ordering. Notice that in all cases we have $V_s^a \leq W_t^b$ if and only if $W_t^{\neg b} \leq V_s^{\neg a}$. As there are a finite number of these subspaces, there must exist at least one maximal element and at least one minimal element with respect to the partial order. Given that $V_s^a \leq W_t^b$ if and only if $W_t^{\neg b} \leq V_s^{\neg a}$, it holds that V_s^a is maximal if and only if $V_s^{\neg a}$ is minimal, and similarly for W_t^b versus $W_t^{\neg b}$.

Now, we claim that it is possible to reassign all maximal and minimal subspaces to $\mathcal{A}$ or $\{0\}$ in such a way that (i) $V_s^a = \mathcal{A}$ if and only if $V_s^{\neg a} = \{0\}$ (and similarly for W_t^b versus $W_t^{\neg b}$), and (ii) the partial ordering is preserved. If V_s^a is maximal but not minimal, then $V_s^{\neg a}$ is minimal and

not maximal, so it is clear that reassigning $V_s^a = \mathcal{A}$ and $V_s^{\neg a} = \{0\}$ satisfies these conditions. In case V_s^a is both maximal and minimal, then the partial ordering is essentially behaving trivially with respect to V_s^a (possibly equating V_s^a with other subspaces). In this case we set V_s^a and $V_s^{\neg a}$ to $\mathcal{A}$ and $\{0\}$ arbitrarily, provided spaces equated with V_s^a or $V_s^{\neg a}$ are assigned accordingly. The situation is similar for W_t^b and $W_t^{\neg b}$. Applying this reassignment recursively to the remaining subspaces (the ones that were neither maximal or minimal) eventually reassigns all subspaces to $\{0\}$ or $\mathcal{A}$. The partial ordering is preserved and the reassignments necessarily satisfy $V_s^a = (V_s^{\neg a})^\perp$ and $W_t^b = (W_t^{\neg b})^\perp$ for all choices of s, t, a, and b.

At this point a perfect deterministic strategy may be derived. Specifically, if $V_s^a = \mathcal{A}$, then Alice answers question s with a, and otherwise if $V_s^a = \{0\}$ then Alice answers $\neg a$. Bob's answers are similarly determined by the (reassigned) subspaces $\{W_t^b\}$. As one of V_s^0 and V_s^1 is set to $\mathcal{A}$ and the other to $\{0\}$, and similarly for W_t^0 and W_t^1, this strategy is well-defined. The strategy can be seen to be a perfect strategy because Alice and Bob have zero probability to answer incorrectly—if (s,t,a,b) satisfy $\pi(s,t) > 0$ and $V(a,b\,|\,s,t) = 0$, then the fact that the partial order was preserved implies that $V_s^a \subseteq W_t^{\neg b}$ and $W_t^b \subseteq V_s^{\neg a}$. Thus, we cannot have $V_s^a = \mathcal{A}$ and $W_t^b = \mathcal{A}$, and therefore Alice and Bob do not answer the pair of questions (s,t) incorrectly with answers (a,b).

It remains to show that a perfect quantum strategy implies the existence of subspaces $\{V_s^a\}$ and $\{W_t^b\}$ as above. We may assume without loss of generality that Alice and Bob use a strategy satisfying the properties given by Theorem 5.4. As in the proof of Theorem 5.4, let

$$Z_t^b = \mathrm{tr}_{\mathcal{B}}(I \otimes Y_t^b)|\psi\rangle\langle\psi|$$

for each $t \in T$ and $b \in \{0,1\}$. We have

$$\sum_{s,t,a,b} \pi(s,t) V(a,b\,|\,s,t)\,\mathrm{tr}(X_s^a Z_t^b) = 1$$

where $\{X_s^a : s \in S, a \in \{0,1\}\}$ are projections with $X_s^0 + X_s^1 = I$ for each $s \in S$, and $\{Z_t^b : t \in T, b \in \{0,1\}\}$ are positive semidefinite matrices with $Z_t^0 + Z_t^1 = \rho = \mathrm{tr}_{\mathcal{B}}\,|\psi\rangle\langle\psi|$ for each $t \in T$.

Now, note that for any choice for positive semidefinite matrices $\{Z_t^b : t \in T, b \in \{0,1\}\}$ satisfying $Z_t^0 + Z_t^1 = \rho$ for each $t \in T$, we have that the quantity

$$\sum_{s,t,a,b} \pi(s,t)\,\mathrm{tr}(X_s^a Z_t^b)$$

is at most 1, and therefore the quantity

$$\sum_{s,t,a,b} \pi(s,t) V(a,b\,|\,s,t)\,\mathrm{tr}(X_s^a Z_t^b) \qquad (5)$$

is also at most 1. Therefore, by Lemma 5.5 we may replace the matrices $\{Z_t^b\}$ by new matrices satisfying $Z_t^0 + Z_t^1 = \rho$ and $\mathrm{tr}(Z_t^0 Z_t^1) = 0$ while still achieving the maximum value of 1 in Eq. 5. (These new matrices do not necessarily arise from some different strategy for Bob, but this is irrelevant.)

Let V_s^0 and V_s^1 be the orthogonal spaces onto which X_s^0 and X_s^1, respectively, are projections, and let W_t^0 and W_t^1 be the spaces representing the span of the nonzero eigenvectors of Z_t^0 and Z_t^1, respectively. Because X_s^0 and X_s^1 are orthogonal projections with $X_s^0 + X_s^1 = I$ and because Z_t^0 and Z_t^1 satisfy $\mathrm{tr}(Z_t^0 Z_t^1) = 0$ and $Z_t^0 + Z_t^1 = \rho = \mathrm{tr}_{\mathcal{B}}\,|\psi\rangle\langle\psi|$, we have that the first required property of the spaces $\{V_s^a\}$ and $\{W_t^b\}$ is satisfied. The fact that the second property is satisfied follows from the fact that the value of Eq. 5 is 1 and therefore

$$\sum_{s,t,a,b} \pi(s,t)(1 - V(a,b\,|\,s,t))\,\mathrm{tr}(X_s^a Z_t^b) = 0,$$

implying that $\mathrm{tr}(X_s^a Z_t^b) = 0$ whenever $\pi(s,t) > 0$ and $V(a,b\,|\,s,t) = 0$. This completes the proof. ■

5.4. Bounds on entanglement for XOR games

The final results we prove concern the *amount* of entanglement needed for Alice and Bob to play a given game optimally. With respect to this question, our results are restricted to XOR games. The following theorem follows immediately from the results of Section 5.2.

Theorem 5.13. *Let G be an XOR game and let $N = \min(|S|,|T|)$. There exists an optimal strategy for Alice and Bob for G in which they share a maximally-entangled state on $\lceil N/2 \rceil$ qubits.*

Unfortunately, even in this restricted setting of XOR games, the bound on the amount of entanglement provided by this theorem is still huge—the number of qubits shared by Alice and Bob is exponential in the sizes of their inputs.

However, if we are willing to settle for a slightly suboptimal strategy, a polynomial number of shared qubits suffices. This fact follows from the Johnson-Lindenstrauss lemma [27], which we now state, following Ref. [14].

Lemma 5.14 (Johnson-Lindenstrauss). *For $\varepsilon \in (0,1)$ and n a positive integer, let K be a positive integer such that*

$$K \geq 4\left(\varepsilon^2/2 - \varepsilon^3/3\right)^{-1} \log n.$$

Then for any set V of n points in $\mathbb{R}^d$, there is a mapping $f : \mathbb{R}^d \to \mathbb{R}^K$ such that for all $u, v \in V$,

$$(1-\varepsilon)||u-v||^2 \leq ||f(u) - f(v)||^2 \leq (1+\varepsilon)||u-v||^2.$$

Theorem 5.15. *Let $G = G(V, \pi)$ be an XOR game with quantum value $\omega_q(G)$. Let $0 < \varepsilon < 1/10$, and suppose K is an even integer such that*

$$K \geq 4\left(\varepsilon^2/2 - \varepsilon^3/3\right)^{-1} \log\left(|S| + |T| + 1\right).$$

Then, if Alice and Bob share a maximally entangled state on $K/2$ qubits, they can win with probability greater than $\omega_q(G) - \varepsilon$.

Proof. Let $M = |S| + |T|$ and $0 < \varepsilon < 1/10$. Let $x_1, \ldots, x_{|S|}, y_1, ..., y_{|T|}$ be the vectors associated with the optimal quantum strategy according to Proposition 5.7. Apply the Johnson-Lindenstrauss Lemma to the $M + 1$ points $x_1, \ldots, x_{|S|}, y_1, \ldots, y_{|T|}$, and $\vec{0}$. Set

$$x'_s = \frac{f(x_s) - f(\vec{0})}{||f(x_s) - f(\vec{0})||} \quad \text{and} \quad y'_t = \frac{f(y_t) - f(\vec{0})}{||f(y_t) - f(\vec{0})||}.$$

for each $s \in S$ and $t \in T$. Because $x \cdot y = 1 - ||x - y||/2$ for real unit vectors x and y, we have

$$|\, x'_s \cdot y'_t - x_s \cdot y_t \,| = \frac{1}{2} \left|\, ||x'_s - y'_t|| - ||x_s - y_t|| \,\right|.$$

A straightforward calculation based on the fact that

$$\sqrt{1-\varepsilon} \leq ||f(x_s) - f(\vec{0})|| \leq \sqrt{1+\varepsilon},$$
$$\sqrt{1-\varepsilon} \leq ||f(y_t) - f(\vec{0})|| \leq \sqrt{1+\varepsilon},$$

and

$$\sqrt{1-\varepsilon}||x_s - y_t|| \leq ||f(x_s) - f(y_t)|| \leq \sqrt{1+\varepsilon}||x_s - y_t||$$

proves that

$$\frac{1}{2} \left|\, ||x'_s - y'_t|| - ||x_s - y_t|| \,\right| < 2\varepsilon.$$

We note that these vectors can be realized as a quantum strategy by Theorem 5.6. It follows that the difference in the probability of winning using this strategy instead of the optimal one is

$$\frac{1}{2} \sum_{s,t} \pi(s,t) \left[V(0\,|\,s,t) - V(1\,|\,s,t)\right] (x_s \cdot y_t - x'_s \cdot y'_t)$$
$$\leq \frac{1}{2} \sum_{s,t} \pi(s,t) \, |x_s \cdot y_t - x'_s \cdot y'_t| \leq \epsilon \sum_{s,t} \pi(s,t) = \varepsilon.$$

Hence Alice and Bob win using this strategy with probability greater than $\omega_q(G) - \varepsilon$. ∎

Theorem 5.15 implies that any protocol for an XOR-game can be simulated with success probability within precision ε using an amount of entanglement that scales polynomially with respect to $\log |S|$, $\log |T|$, and $1/\varepsilon$. Combining this result with one in [29], we obtain the following.

Corollary 5.16. *For all s and c such that $0 \leq s < c \leq 1$, $\oplus\text{MIP}^*_{c,s}[2] \subseteq \text{NEXP}$.*

We have no lower bounds on the amount of entanglement required to play XOR games optimally or near optimally. Perhaps even a *constant* amount of entanglement is sufficient.

Acknowledgments

We would like to thank Andris Ambainis, Dave Bacon, Anne Broadbent, Andrew Doherty, Nicolas Gisin, David Mermin, Asher Peres, John Preskill, Madhu Sudan, and Alain Tapp for helpful discussions, Steven Finch for providing us with copies of Refs. [15] and [38], and the anonymous referees for several helpful comments and corrections. This work was partially supported by Canada's NSERC, MITACS, PIMS, CIAR, the U.S. National Science Foundation under Grant No. EIA-0086038, and Alberta's iCORE.

References

[1] N. Alon and A. Naor. Approximating the cut-norm via Grothendieck's inequality. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, 2004.

[2] A. Ambainis, 2001. Personal communication.

[3] P. K. Aravind. The magic squares and Bell's theorem. Manuscript, 2002. arXiv.org e-Print quant-ph/0206070.

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

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

[6] M. Bellare, O. Goldreich, and M. Sudan. Free bits, PCPs, and non-approximability — towards tight results. *SIAM Journal on Computing*, 27(3):804–915, 1998.

[7] 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.

[8] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[9] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999.

[10] S. Braunstein and C. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202:22–56, 1990.

[11] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 63–68, 1998.

[12] 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.

[13] 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.

[14] S. Dasgupta and A. Gupta. An elementary proof of the Johnson-Lindenstrauss lemma. Technical Report TR-99-006, International Computer Science Institute, Berkeley, California, 1999.

[15] A. M. Davie. Lower bound for K_G. Unpublished note, 1984.

[16] 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.

[17] 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.

[18] S. R. Finch. *Mathematical Constants*. Cambridge University Press, 2003.

[19] P. Fishburn and J. Reeds. Bell inequalities, Grothendieck's constant, and root two. *SIAM Journal on Discrete Mathematics*, 7:48–56, 1994.

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

[21] P. Frankl and V. Rodl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

[22] V. Galliard, A. Tapp, and S. Wolf. The impossibility of pseudo-telepathy without quantum entanglement. arXiv.org e-Print quant-ph/0211011, 2002.

[23] M. X. Goemans and D. P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42:1115–1145, 1995.

[24] A. Grothendieck. Résumé de la théorie métrique des produits tensoriels topologiques. *Boletim Da Sociedade de Matemática de São Paulo*, 8:1–79, 1953.

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

[26] P. Heywood and M. L. G. Redhead. Nonlocality and the Kochen-Specker paradox. *Foundations of Physics*, 13:481–499, 1983.

[27] W. Johnson and J. Lindenstrauss. Extensions of Lipschitz maps into a Hilbert space. *Contemporary Mathematics*, 26:189–206, 1984.

[28] L. A. Khalfin and B. S. (Tsirelson) Tsirel'son. Quantum and quasi-classical analogs of Bell inequalities. In P. Lahti and P. Mittelstaedt, editors, *Symposium on the Foundations of Modern Physics*, pages 441–460. World Scientific, 1985.

[29] 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.

[30] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967.

[31] J. L. Krivine. Constantes de Grothendieck et fonctions de type positif sur les sphères. *Advances in Mathematics*, 31:16–30, 1979.

[32] D. Lapidot and A. Shamir. Fully parallelized multi prover protocols for NEXP-time. In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 13–18, 1991.

[33] N. D. Mermin. Simple unified form for no-hidden variables theorems. *Physical Review Letters*, 65:3373–3376, 1990.

[34] N. D. Mermin. Hidden variables and the two theorems of John Bell. *Reviews of Modern Physics*, 65(3):803–815, 1993.

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

[36] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer, 1993.

[37] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[38] J. A. Reeds. A new lower bound on the real Grothendieck constant. Unpublished note, 1991.

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

[40] B. S. (Tsirelson) Tsirel'son. Quantum analogues of the Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.

[41] L. Vaidman. Tests of Bell inequalities. arXiv.org e-Print quant-ph/0107057, 2001.