Non-Local Correlations and Interactive Games

Daniel Ciprian Preda

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2011-64
http://www.eecs.berkeley.edu/Pubs/TechRpts/2011/EECS-2011-64.html

May 17, 2011

Non-Local Correlations and Interactive Games

by

Daniel Ciprian Preda

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Engineering - Electrical Engineering and Computer Sciences

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Umesh Vazirani, Chair
Professor Satish Rao
Professor Michael Crommie

Spring 2011

The dissertation of Daniel Ciprian Preda, titled Non-Local Correlations and Interactive Games, is approved:

Chair _____ Date _____

_____ Date _____

_____ Date _____

University of California, Berkeley

Abstract

Non-Local Correlations and Interactive Games

by

Daniel Ciprian Preda

Doctor of Philosophy in Engineering - Electrical Engineering and Computer Sciences

University of California, Berkeley

Professor Umesh Vazirani, Chair

Quantum entanglement, and the resulting peculiar non-classical correlations are one of the most counter-intuitive aspects of quantum mechanics.

The formalism of interactive games from computational complexity theory provides a useful framework in which to understand the power of entanglement. In an interactive game, a verifier interacts with a number of infinitely powerful provers who are allowed to share quantum entanglement but otherwise can't communicate. The ability of the verifier to extract useful information from the provers, whom he does not trust, provides an interesting measure of the ability of the provers to coordinate using their shared entanglement. Two particular interactive games we'll look at are Magic Square and 3SAT.

The Magic Square game is the iconic example of a game where two classical provers cannot perfectly coordinate their strategies using shared randomness, but quantum provers with shared entanglement can win with probability 1. We show that by adding an extra prover, we disallow perfect cheating. For 3SAT with three provers we also show that perfect cheating is not possible.

We then generalize the results for Magic Square and 3SAT by looking at non-commuting provers, a superset of entangled provers (communication is allowed, but operators applied by different provers must commute). Using this method, we obtain a generalized Tsirelson inequality that we apply to the Magic Square. Hence, we are able to give provably optimal strategies for the general Magic Square with n players. We also recover a similar result for 3SAT as with entangled provers, and we improve on it by showing that the gap is inverse exponential in the input size.

The no-signaling principle, which forbids faster than light communication, is a fundamental constraint on the non-local correlations resulting from quantum entanglement. However, no-signaling allows distributions that are more general than those arising from quantum mechanics. In particular, using a specific "unit" of general non-local correlation (the Popescu-Rohlich box), we show that there are classes that are equal to **NEXP** classically, but collapse to **AM** once such correlations are allowed. We also show that **MIP** where the verifier only looks at the XOR of the answers collapses to **PSPACE**. For the second approach, we show that by writing general non-local correlations as linear constraints, **MIP** is included in **EXP** under such correlations (vs **NEXP** classically).

We can extend these results to entangled quantum provers, by formulating an artificial **MIP**-like class built on a promise problem, that classically is equal to **NEXP**, but that also collapses to **AM** when quantum correlations are present.

Dedication

This dissertation is dedicated to my parents Mircea and Viorica who have supported me all the way since the beginning of my studies. Also, this thesis is dedicated to my wife Loulena, without whose encouragement this work may have never been completed.

Contents

Acknowledgements

I want to thank Barbara Terhal for introducing me to the world of non-signaling correlations, and for a wonderful internship experience. I am forever grateful to my advisor Umesh Vazirani for guiding me toward completing my degree, stimulating discussions, insightful remarks and helping me see the bigger picture. I want to thank Andrew Yao and Xiaoming Sun for a memorable and fruitful year in China, Michael Crommie and Satish Rao for being part of my dissertation committee, and Thomas Vidick for useful discussions about quantum entanglement.

Chapter 1

Introduction

Entanglement is a fundamental resource in Quantum Theory. One of the first examples that touched on its power is the famous EPR experiment. It can be simply described by two spatially separated particles whose individual states are random, and yet once we measure one particle, the state of the other one is precisely determined.

By performing measurements on an entangled quantum system, two separate observers can obtain correlations that are nonlocal, in the sense that the joint probabilities $P(a_1, a_2|x_1, x_2)$ for the observers to get the outcomes a_1 and a_2 given the measurements x_1 and x_2 cannot be written as a convex combination of marginal probability distributions. The nonlocal character of the correlations implies that two parties who wish to simulate the experiment with only classical resources, cannot do so without communication. Nonlocal correlations, although they cannot be used to signal from one observer to the other, can be exploited in various information processing tasks, such as in communication complexity or for the distribution of a secret key between two parties..

The non-local correlations obtained through entanglement have subtle properties which can be better understood by studying them in the context of interactive proofs / games. This is the focus of this dissertation. In an interactive proof, a verifier, with limited computational power, needs to decide whether a specific input problem has a certain property. To this end, it interacts with two or more computationally unbounded provers (players) by asking them questions. The provers cannot communicate during the protocol, but they can agree beforehand on a strategy and/or share correlations in order to implement that strategy. It is the absence of communication that allows the verifier to obtain any confidence in the answers of the provers, each of whom it distrusts individually. It is in this sense that the provers ability to mislead the verifier is a subtle measure of the non-local correlations achievable through shared entanglement.

Two interactive games of particular interest are the Magic Square and 3SAT. The Magic Square is an example of a game in which two entangled provers can cheat perfectly, while classical provers have a non-zero probability of being caught. 3SAT is the canonical interactive proof game in complexity theory. Moreover, the Magic Square can be cast as a 3SAT game. This implies that, in some instances, the 3SAT verifier can also be misled with probability 1 by entangled provers. The focus of the first part of this dissertation is to modify those two protocols in such a way as

to prohibit perfect cheating. We will accomplish this by adding a third prover to each game, and drawing on the intuition brought by the monogamy of entanglement principle: if two systems are strongly correlated, then they cannot be strongly correlated with a third system too.

We will show that by adding a third prover there are no cheating strategies. The main result for the Magic Square is derived from a 3-party Tsirelson-like bound, which can be seen as a generalization of the Bell inequality, and that limits the provers ability to mislead the verifier. For the 3SAT game, we show that the shared state of any quantum strategy that wins with probability 1 can be written as a superposition of states that correspond to ± 1 eigenvalues of the operators applied by each party. Those eigenvalues correspond to a classical satisfying assignment, and hence the formula is satisfiable.

In the second part of this dissertation, we consider a generalization of the entangled provers by considering provers that can communicate, but the operators applied by different provers have to commute. Any winning strategy that is entangled can be written by default as a commuting prover strategy. Although these provers may be able to mislead the verifier more easily, we know that any upper bound on the winning probability would apply to the entangled provers as well. Again, we will study the Magic Square and 3SAT problems under this formalism.

By taking into account the commuting properties of the operators, we first derive a generalized Tsirelson-like inequality for n parties. We also show that solving a general Magic Square problem is equivalent to solving a symmetric version of a specific Magic Square instance, where provers are queried in a predetermined manner. By combining these two facts, we obtain an upper bound on the probability of wining in a Magic Square game with n players. Finally, we give an explicit entangled strategy that achieves this bound.

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 introduced by Hastad. In the PCP formalism, instead of the verifier actively interacting with a number of provers, it can look up certain bits from a (long, pre-written) proof in order to convince itself of a certain fact. In our protocol, the verifier will perform, with equal probability, either a consistency test (send the same question to all provers and check for consistent answers), or a simulation test (behave in the same way as the PCP verifier).

We first give a simpler proof to the fact that if there is no satisfying assignment, then no perfect cheating is possible. The result is based on the intuitive fact that if there is a strategy that achieves probability 1, then all operators commute. Thus, they can be simultaneously diagonalized, and the resulting eigenvalues correspond to a classical assignment. Next, we prove that the soundness gap is at least inverse exponential in the size of the input. We start with the method introduced by Kempe et all [25] but instead of using the non-disturbance property, we modify the proof to take into account the fact that all the POVMs almost commute. The basic idea is that if the consistency test is passed with high probability, then the provers cannot cheat too much on the simulation test.

In the final part of this dissertation, we contrast quantum entanglement and non-local correlations in general. In particular, it is possible to write down sets of non-signaling correlations that are more non-local than allowed by quantum mechanics [4].

In this spirit, it is useful to consider non-local correlations that do not necessarily arise from a set of measurements on a quantum state. Suppose that two observers have access to a black box. When an observer i introduces an input x_i , the box produces an output a_i . The box is characterized by the joint probability $P(a_1, a_2|x_1, x_2)$ of obtaining the output pair (a_1, a_2) given the input pair (x_1, x_2). Compatibility with special relativity requires that these joint probabilities satisfy the no-signaling conditions

$$\sum_{a_2} P(a_1, a_2|x_1, x_2) = \sum_{a_2} P(a_1, a_2|x_1, x_2^{'}) = P(a_1|x_1)$$

for all $a_1, x_1, x_2, x_2^{'}$, as well as a similar set of conditions obtained by summing over the first observer's outputs. This ensures that one observer cannot signal to the other via his choice of input in the box. Apart from these constraints, the joint distribution can be arbitrary and, in particular, nonlocal. The definition of nonlocal boxes generalizes to more parties in a straightforward way.

A central question is whether these stronger-than-quantum correlations exist or not in nature. While we can't answer directly, we will start by bringing arguments showing that the existence of such correlations has profound implications for complexity theory. We will show that general correlations are strong, and in some cases so strong that they can simulate communication among provers in the context of interactive proofs. We start by looking at the most general non-local correlations, and we prove two sets of results based either on specific instances of such correlations, or on arbitrary classes.

Popescu-Rohlich boxes (PR) are one particular instance of a non-local box. In particular, for two parties, on input bits x and y, the box outputs bits a and b respectively, such that $a \oplus b = x \cdot y$. We show that two or more parties that share an unlimited number of Popescu-Rohlich non-local boxes can simulate communication from the point of view of a verifier who only looks at the (bitwise) XOR of the answers (i.e. the XOR of their answers can be the same as the XOR of the answers given by any provers who are allowed to communicate). Hence from the point of view of the verifier there is only one prover, which leads to several class collapses (the most notable being that there is a class that classically is equal to **NEXP** but that collapses to **AM** under such correlations)

We then proceed by writing general correlations as linear equations involving the non-signaling constraints. We can build a linear program that can be solved in exponential time and that approximates the value of the game. Hence, we can prove that **MIP** $\in$ **EXP** whenever the provers share non-local correlations.

Finally, we show that we can build a "fake" three-party PR box using a quantum GHZ state and a promise problem. This leads to the existence of an artificial class that classically is equal to **NEXP** but that also collapses to **AM** under quantum correlations. However, although this class is **MIP**-like, it requires the presence of a "trusted" prover (i.e. a prover that has a fixed behavior) in order to satisfy the promise problem.

Chapter 2

Quantum Entanglement

An intriguing open question in quantum complexity is whether quantum multi-prover systems with prior entanglements have the same language recognition power as the classical multi-prover systems. This appears to be a subtle question, and the standard way of utilizing the two provers in the classical case turns out to allow, for some problems such as the Magic Square game, the provers in the quantum case to cheat a classical verifier successfully with probability 1. In this chapter we investigate the performance of a natural interactive quantum protocol for 3-SAT using three quantum provers and a classical verifier. First, we show that for the Magic Square game, the probability of quantum provers to cheat successfully is at most $(2 + \sqrt{3})/4$. The key to the proof is the establishment of a novel cubic polynomial Tsirelson-type inequality of independent interest, which puts constraints on genuinely triple quantum correlations among 3 entangled parties. Second, for any general unsatisfiable 3- SAT instance, we show that the quantum provers cannot cheat successfully with probability 1. These results are encouraging, leaving open the possibility that, with a better analysis of the success probability, the protocol may provide a valid quantum 3-prover system for any language in NEXP, just as in the classical case.

2.1 Introduction

Quantum multi-prover interactive systems were defined in Kobayashi and Matsumoto [27], where it was shown that they recognize exactly the class of languages NEXP, if the quantum provers do not share prior entanglements. It is an intriguing open question whether this remains true when the provers are allowed to be in an entangled initial state.

A natural quantum 2-prover strategy would be to convert the problem into a 3-SAT instance, pick a random clause, ask prover 1 to give the assignments of the literals in the clause, ask prover 2 to give the value of a random literal in the clause, and then check for consistency. Unfortunately, there are examples for which two entangled quantum provers can cheat successfully with certainty as discussed below.

Cleve, Hoyer, Toner and Watrous [11] initiated a study of the power of entangled quantum

2-prover systems, using to their advantage the linkage between this topic and quantum games for which there is a substantial literature. In particular it was pointed out that the well-known quantum Magic Square game provides an easy example of a 3-SAT instance where 2 classical provers cannot cheat successfully all the time, while 2 entangled quantum provers can. (Another such example based on graph coloring was credited to Ambainis in [11].) The paper [11] established a wealth of results regarding quantum 2-prover systems. But there does not seem to be any good candidate left as potential entangled quantum 2-prover systems to recognize all languages in NEXP.

In this chapter we investigate the performance of a natural interactive quantum protocol for 3-SAT using three quantum provers and a classical verifier, where the provers share entanglement. First, we show that for the Magic Square game, the probability of quantum provers to cheat successfully is at most $(2+\sqrt{3})/4$. The key to the proof is the establishment of a novel cubic polynomial Tsirelson-type inequality, which may be of independent interest. Second, for any general unsatisfiable 3-SAT instance, we show that the quantum provers cannot cheat successfully with probability 1. These results are encouraging, leaving open the possibility that, with a better analysis of the success probability, the protocol may provide a valid quantum 3-prover system for any language in NEXP, just as in the classical case.

Note that one can consider an analogous quantum 2-prover system for 2-SAT. The results in [11] implies that, for unsatisfiable 2-SAT instances, the 2 quantum provers cannot cheat successfully with probability 1. Our second result above can be regarded as a non-trivial extension of this.

We remark that the verifier is a classical machine in the quantum multi-prover model in [11], in contrast to that in [27]. This does not affect our current discussion since we are focusing on the analysis of specific protocols which happen to have classical verifiers.

Related work: Kempe and Vidick [23] give a 2-prover quantum interactive proof system for GAP-3D-MATCHING with perfect completeness and soundness $1-2^{-O(n)}$, where the provers share entanglement. In their system the verifier and the communication are also quantum. Independently Ben Toner [36] and Kobayashi and Matsumoto [26] show that languages in NP have a 3-prover quantum interactive proof system with completeness c and soundness s such that $c-s = 1/poly(n)$. Their protocols try to simulate the classical 2-prover proof system for NP by three quantum provers. They are quite different from our protocol.

2.2 Main Result

As in [11], we phrase the results in the quantum game terminology. Its connection to quantum 3-prover system is clear.

Let V be a predicate on a finite set $S \times T \times U \times A \times B \times C$, and let π be a probability distribution on $S \times T \times U$. The game $G(V,\pi)$ is played as follows: A triplet of questions $(s,t,u) \in S \times T \times U$ is randomly chosen according to π, and s,t,u are sent to players 1, 2, 3, respectively. The players then respond with answers $a \in A, b \in B, c \in C$. The players win if $V(s,t,u,a,b,c) = 1$, and lose otherwise. The players are not allowed to communicate after the questions are received, but they

may plan on strategies prior to receiving their questions. For convenience, we shall call the players Alice, Bob, and Charlie.

The classical value of a game $G = G(V, \pi)$ is the maximum probability with which the players can win the game, using purely classical strategies. Denote it by $\omega_c(G)$. Clearly, the optimal value can be achieved using some deterministic strategy in which a, b, c are simply functions of s, t, u, respectively. Thus,

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

A quantum strategy is specified by an initial tripartite state $|\psi\rangle$ shared by Alice, Bob and Charlie, a quantum measurement for Alice for each $s \in S$, a quantum measurement for Bob for each $t \in T$, and a quantum measurement for Charlie for each $u \in U$. Each player receives an input, performs the associated measurement on its portion of the state $|\psi\rangle$, and sends back the measured value. The quantum value of a game $G = G(V, \pi)$ is the maximum probability with which the players can win the game. Call this value $\omega_q(G)$.

Starting with the original Bell inequalities, there are many known constraints on the amount of correlation achievable in both the classical and the quantum realms. Notable among these are the CHSH inequality [9] and Tsirelson inequality [38] [39].

Let Alice and Bob be two separate parties sharing a quantum state $|\psi\rangle$. Let A_1, A_2 be Alice's observables and Hermitian operators with eigenvalues $1, -1$. Similarly, B_1, B_2 are Bob's observables and are Hermitian operators with eigenvalues $1, -1$. Let $\langle A_j B_k \rangle = \langle \psi | A_j \otimes B_k | \psi \rangle$. Tsirelson inequality states

$$|\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle| \leq 2\sqrt{2}$$

As comparison, the CHSH inequality states that if Alice and Bob are classical players, then the correlation is considerably more stringent

$$|\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle| \leq 2$$

These inequalities have been the subjects of much study in recent years, and have played an important role in the analysis of $\omega_c(G), \omega_q(G)$.

2.2.1 3-player Magic Square Game

Our first result relates to a special game which is called the Magic Square game [1] [29] [30] [11]. The basic idea is that there does not exist a 3 by 3 $0 - 1$ matrix such that each row has even parity and each column has odd parity. In this game the verifier randomly picks a row or a column and

asks Alice to fill in the values of the entries and checks the parity, then randomly picks one of the three entries given to Alice and asks Bob to fill in the value, and then checks the consistency of the answers given by Alice and Bob. It has been shown that for this game there exists a quantum strategy for Alice and Bob to cheat perfectly, i.e. $\omega_q(G) = 1$ for this game.

Here we consider the magic square game with three players. There are three players: Alice, Bob and Charlie. The verifier randomly picks a row or a column, and randomly asks Alice, Bob and Charlie the value of a different entry in that row or column, and then checks the parity of the answers. It is not hard to see that the classical value of this game is $\omega_c(G) = 5/6$. We will prove $\omega_q(G) \leq (2 + \sqrt{3})/4$, i.e. Alice, Bob and Charlie cannot perfectly cheat even by using a quantum strategy. The key point is the following novel Tsirelson-type inequality. It gives constraints on the amount of genuine triple quantum correlations among three parties, instead of the usual two parties, and should be of independent interest.

Alice, Bob, and Charlie are three separate parties sharing a quantum state $|\psi\rangle$. Let A_1, A_2, A_3 be Alice's observables and are Hermitian operators with eigenvalues $1, -1$. Simi- larly, B_1, B_2, B_3 (C_1, C_2, C_3) are Bob's (Charlie's) observables and are Hermitian operators with eigenvalues $1, -1$. Let $\langle A_j B_k C_l\rangle = \langle\psi|A_j \otimes B_k \otimes C_l|\psi\rangle$.

Theorem 2.2.1.

$$|A_1B_2C_3 + A_2B_3C_1 + A_3B_1C_2 - A_1B_3C_2 - A_2B_1C_3 - A_3B_2C_1| \leq 3\sqrt{3}$$

where A_j, B_j, C_k are observables of Alice, Bob and Charlie.

Corollary 2.2.2. *For 3-player magic square game G, $\omega_q(G) \leq (2 + \sqrt{3})/4$*

In the literature, there have been suggestions of an even wider class of nonlocal but still non-signalling strategies, starting with Popescu and Rohrlich [34](also see e.g., [4]). Let $\omega_{ns}(G)$, the nonlocal value of a game G denote the maximum possible probability that players can win the game with such strategies. Clearly, $\omega_{ns}(G) \geq \omega_q(G) \geq \omega_c(G)$. The quantity $\omega_{ns}(G)$ has the advantage of having certain linear programming characterizations, and there are situations when $\omega_q(G)$ can be determined by showing $\omega_{ns}(G) = \omega_c(G)$. Our next result shows that this cannot be the case here. In fact we show that there exists a nonlocal box such that Alice, Bob and Charlie can be correlated perfectly:

Theorem 2.2.3. *For 3-player magic square game G, $\omega_{ns}(G) = 1$.*

2.2.2 3-SAT Game

Our second result concerns a general 3-player binary game, we call it 3-SAT game: Alice, Bob, and Charlie would like to convince the verifier that a 3-CNF boolean formula f is satisfiable. The verifier first randomly picks a clause, and then with $1/2$ probability randomly picks a variable in that clause and asks Alice, Bob and Charlie the value of this variable, then checks the consistency of the answers, or with $1/2$ probability randomly asks Alice, Bob and Charlie each one a different variable in that clause, then checks the satisfiability of the clause. We have the following theorem:

Theorem 2.2.4. *Let f be a 3-CNF boolean formula and G be the corresponding 3-SAT game, then $\omega_q(G) = 1$ iff $\omega_c(G) = 1$, i.e. f is satisfiable.*

Remark: Let n be the number of variables in f , then actually we can bound $\omega_q(G) < 1 - \exp(-2cn)$, if assume $\omega_c(G) < 1$, i.e., $NP \subseteq MIP^*_{\log n}(3, 1, 1, 1 - \exp(-2cn))$.

2.3 Proof of Theorem 3.2.1

Let

$$A = \begin{bmatrix} 0 & A_3 & -A_2 \\ -A_3 & 0 & A_1 \\ A_2 & -A_1 & 0 \end{bmatrix}, F = A_3A_1A_2 - A_2A_1A_3$$

The structure of A's eigenvalues and corresponding eigenvectors is as follows:

Since F is skew-hermitian, we can write $F = i\sum_j \eta_j |u_j\rangle\langle u_j|$, $i\eta_j$ is an eigenvalue ($\eta_j \in R$) and $|u_j$ is the corresponding eigenvector, $\{|u_j : j = 1, ..., n\}$ form an orthonormal basis of the space.

For each j:

(1) if $|\eta_j| < 2$, define $\lambda_{j,1}, \lambda_{j,2}, \lambda_{j,3}$ as the three roots of equation $z(3 - z^2) = \eta_j$ (this equation has three real roots when $-2 \le \eta_j \le 2$), and three $3n$-dimension vectors

$$v_{j,l} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ \frac{1}{1-\lambda_{j,l}^2}(A_1A_2 - i\lambda_{j,l}A_3)|u_j\rangle \\ \frac{1}{1-\lambda_{j,l}^2}(A_1A_3 + i\lambda_{j,l}A_2)|u_j\rangle \end{bmatrix}, l = 1, 2, 3$$

(2) If $\eta_j = 2$, define $\lambda_{j,1} = -2, \lambda_{j,2} = 1, \lambda_{j,3} = 1$, and

$$v_{j,1} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ -iA_3|u_j\rangle \\ iA_2|u_j\rangle \end{bmatrix}, v_{j,2} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ e^{i\frac{\pi}{6}}A_3|u_j\rangle \\ e^{-i\frac{\pi}{6}}|u_j\rangle \end{bmatrix}, v_{j,2} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ e^{i\frac{5\pi}{6}}A_3|u_j\rangle \\ e^{-i\frac{5\pi}{6}}A_2|u_j\rangle \end{bmatrix}$$

(3) If $\eta_j = -2$, define $\lambda_{j,1} = 2, \lambda_{j,2} = -1, \lambda_{j,3} = -1$, and

$$v_{j,1} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ iA_3|u_j\rangle \\ -iA_2|u_j\rangle \end{bmatrix}, v_{j,2} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ e^{-i\frac{\pi}{6}}A_3|u_j\rangle \\ e^{i\frac{\pi}{6}}|u_j\rangle \end{bmatrix}, v_{j,2} = \frac{1}{\sqrt{3}} \begin{bmatrix} |u_j\rangle \\ e^{-i\frac{5\pi}{6}}A_3|u_j\rangle \\ e^{i\frac{5\pi}{6}}A_2|u_j\rangle \end{bmatrix}$$

Then $i\lambda_{j,l}$ are eigenvalues of A and $|v_{j,l}\rangle$ are corresponding eigenvectors ($j = 1, ..., n, l = 1, 2, 3$), and $\{|v_{j,1}\rangle, |v_{j,2}\rangle, |v_{j,3}\rangle : j = 1, ..., n\}$ form an orthonormal basis of $3n$-dimension space,

$$A = i\sum_j \lambda_{j,1}|v_{j,1}\rangle\langle v_{j,1}| + \lambda_{j,2}|v_{j,2}\rangle\langle v_{j,2}| + \lambda_{j,3}|v_{j,3}\rangle\langle v_{j,3}|$$

Lemma 2.3.1. *Suppose $\alpha_1, \alpha_2, \alpha_3$ and $\beta_1, \beta_2, \beta_3$ are complex number, $\alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3$, $\eta \in R$, $|\eta| \leq 2$, $\lambda_1, \lambda_2, \lambda_3$ are the three roots of equation $z(3 - z^2) = \eta$. Then*

$$|\Re(i\lambda_1\overline{\alpha_1}\beta_1 + i\lambda_2\overline{\alpha_2}\beta_2 + i\lambda_3\overline{\alpha_3}\beta_3)| \leq \sqrt{3}\sqrt{(|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2)(|\beta_1|^2 + |\beta_2|^2 + |\beta_3|^2)}$$

Remark: The argument is still true if we replace the condition $\alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3$ by $\alpha_1 + \alpha_2 + \alpha_3 = -(\beta_1 + \beta_2 + \beta_3)$. We will use both cases in the proof of the main theorem.

Proof. Since $-2 \leq \eta \leq 2$, we can assume $\eta = 2\sin 3\theta$. From $z(3 - z^2) = \eta$ we know $z \in R$, and $|z| \leq 2$. Let's write $z = 2\sin\gamma$, from $z(3 - z^2) = \eta$ we have $6\sin\gamma - 8\sin^3\gamma = 2\sin 3\theta$, i.e. $\sin 3\gamma = \sin 3\theta$, thus the three roots are:

$$z_1 = 2\sin\theta, z_2 = 2\sin(\theta + \frac{2\pi}{3}), z_3 = 2\sin(\theta - \frac{2\pi}{3})$$

Therefore, $i(\lambda_1\overline{\alpha_1}\beta_1 + \lambda_2\overline{\alpha_2}\beta_2 + \lambda_3\overline{\alpha_3}\beta_3) = 2i\sin\theta\overline{\alpha_1}\beta_1 + 2i\sin(\theta + \frac{2\pi}{3})\overline{\alpha_2}\beta_2 + 2i\sin(\theta - \frac{2\pi}{3})\overline{\alpha_3}\beta_3 = (e^{i\theta} - e^{-i\theta})\overline{\alpha_1}\beta_1 + (e^{i(\theta+\frac{2\pi}{3})} - e^{-i(\theta+\frac{2\pi}{3})})\overline{\alpha_2}\beta_2 + (e^{i(\theta-\frac{2\pi}{3})} - e^{i(\theta-\frac{2\pi}{3})})\overline{\alpha_3}\beta_3$

Let $s = [s_1, s_2, s_3]^T, t = [t_1, t_2, t_3]^T$, where

$$s1 = \frac{1}{\sqrt{3}}(\alpha_1 + \alpha_2 + \alpha_3), s2 = \frac{1}{\sqrt{3}}(\alpha_1 + e^{i\frac{2\pi}{3}}\alpha_2 + e^{-i\frac{2\pi}{3}}\alpha_3), s3 = \frac{1}{\sqrt{3}}(\alpha_1 + e^{-i\frac{2\pi}{3}}\alpha_2 + e^{i\frac{2\pi}{3}}\alpha_3)$$

$$s1 = \frac{1}{\sqrt{3}}(\beta_1 + \beta_2 + \beta_3), s2 = \frac{1}{\sqrt{3}}(\beta_1 + e^{i\frac{2\pi}{3}}\beta_2 + e^{-i\frac{2\pi}{3}}\beta_3), s3 = \frac{1}{\sqrt{3}}(\beta_1 + e^{-i\frac{2\pi}{3}}\beta_2 + e^{i\frac{2\pi}{3}}\beta_3)$$

We can check

$$||s||^2 = |s1|^2 + |s2|^2 + |s3|^2 = |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2$$

$$||t||^2 = |t1|^2 + |t2|^2 + |t3|^2 = |\beta_1|^2 + |\beta_2|^2 + |\beta_3|^2,$$

and

$$i(\lambda_1\overline{\alpha_1}\beta_1 + \lambda_2\overline{\alpha_2}\beta_2 + \lambda_3\overline{\alpha_3}\beta_3) = [\overline{s_1}, \overline{s_2}, \overline{s_3}]\begin{bmatrix} 0 & e^{i\theta} & -e^{-i\theta} \\ -e^{-i\theta} & 0 & e^{i\theta} \\ e^{i\theta} & -e^{-i\theta} & 0 \end{bmatrix}\begin{bmatrix} t_1 \\ t_2 \\ t_2 \end{bmatrix}$$

Since $\alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3$, so $s_1 = t_1$, which implies $\overline{s_1}t_1 \in R, \Re(i\overline{s_1}t_1) = 0$. Thus:

$$\Re(i\lambda_1\overline{\alpha_1}\beta_1 + i\lambda_2\overline{\alpha_2}\beta_2 + i\lambda_3\overline{\alpha_3}\beta_3) = \Re(i\lambda_1\overline{\alpha_1}\beta_1 + i\lambda_2\overline{\alpha_2}\beta_2 + i\lambda_3\overline{\alpha_3}\beta_3) + \sin 3\theta \cdot (i\overline{s_1}t_1)$$

$$\Re\left([\overline{s_1}, \overline{s_2}, \overline{s_3}]\begin{bmatrix} 0 & e^{i\theta} & -e^{-i\theta} \\ -e^{-i\theta} & 0 & e^{i\theta} \\ e^{i\theta} & -e^{-i\theta} & 0 \end{bmatrix}\begin{bmatrix} t_1 \\ t_2 \\ t_2 \end{bmatrix} + \sin 3\theta \cdot (i\overline{s_1}t_1) = \right)$$

$$\Re\left([\overline{s_1}, \overline{s_2}, \overline{s_3}]\begin{bmatrix} i\sin 3\theta & e^{i\theta} & -e^{-i\theta} \\ -e^{-i\theta} & 0 & e^{i\theta} \\ e^{i\theta} & -e^{-i\theta} & 0 \end{bmatrix}\begin{bmatrix} t_1 \\ t_2 \\ t_2 \end{bmatrix}\right)$$

Therefore,

$$|\Re(i\lambda_1\overline{\alpha_1}\beta_1 + i\lambda_2\overline{\alpha_2}\beta_2 + i\lambda_3\overline{\alpha_3}\beta_3)| = \left|\Re\left([\overline{s_1}, \overline{s_2}, \overline{s_3}]\begin{bmatrix} i\sin 3\theta & e^{i\theta} & -e^{-i\theta} \\ -e^{-i\theta} & 0 & e^{i\theta} \\ e^{i\theta} & -e^{-i\theta} & 0 \end{bmatrix}\begin{bmatrix} t_1 \\ t_2 \\ t_2 \end{bmatrix}\right)\right|$$

$$\leq \left|s^\dagger \begin{bmatrix} i\sin 3\theta & e^{i\theta} & -e^{-i\theta} \\ -e^{-i\theta} & 0 & e^{i\theta} \\ e^{i\theta} & -e^{-i\theta} & 0 \end{bmatrix} t\right|$$

Let $Q = \begin{bmatrix} i\sin 3\theta & e^{i\theta} & -e^{-i\theta} \\ -e^{-i\theta} & 0 & e^{i\theta} \\ e^{i\theta} & -e^{-i\theta} & 0 \end{bmatrix}$, then Q is skew-hermitian and the three eigenvalues of Q are $i, i\sqrt{3}, -i\sqrt{3}$. Therefore,

$$|\Re(i\lambda_1\overline{\alpha_1}\beta_1 + i\lambda_2\overline{\alpha_2}\beta_2 + i\lambda_3\overline{\alpha_3}\beta_3)| \leq |s^\dagger Q t| \leq \sqrt{3}||s|| \cdot ||t|| = \sqrt{3}\sqrt{(|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2)(|\beta_1|^2 + |\beta_2|^2 + |\beta_3|^2)}$$

□

Proof of main theorem Let $\widetilde{A_j} = A_j \otimes I \otimes I, \widetilde{B_k} = I \otimes B_k \otimes I, \widetilde{C_l} = I \otimes I \otimes C_l$. To prove the theorem, it is equivalent to prove

$$\langle\psi|(\widetilde{A_1}\widetilde{B_2}\widetilde{C_3} + \widetilde{A_2}\widetilde{B_3}\widetilde{C_1} + \widetilde{A_3}\widetilde{B_1}\widetilde{C_2} - \widetilde{A_1}\widetilde{B_3}\widetilde{C_2} - \widetilde{A_2}\widetilde{B_1}\widetilde{C_3} - \widetilde{A_3}\widetilde{B_2}\widetilde{C_1})|\psi\rangle \leq 3\sqrt{3}.$$

Let $\widetilde{B_j}|\psi\rangle = x_j$ and $\widetilde{C_k}|\psi\rangle = y_k$, here $x_j, y_k \in H_A \otimes H_B \otimes H_C, j, k = 1, 2, 3$. Then the above equation is equivalent to

$$[x_1^\dagger, x_2^\dagger, x_3^\dagger] \begin{bmatrix} 0 & \widetilde{A_3} & -\widetilde{A_2} \\ -\widetilde{A_3} & 0 & \widetilde{A_1} \\ \widetilde{A_2} & -\widetilde{A_1} & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \leq 3\sqrt{3}$$

Write $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, $y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$, and $\widetilde{A} = \begin{bmatrix} 0 & \widetilde{A_3} & -\widetilde{A_2} \\ -\widetilde{A_3} & 0 & \widetilde{A_1} \\ \widetilde{A_2} & -\widetilde{A_1} & 0 \end{bmatrix}$. Since $\widetilde{A_j} = A_j \otimes I \otimes I$, so $\widetilde{A} = A \otimes I \otimes I$, where $A = \begin{bmatrix} 0 & A_3 & -A_2 \\ -A_3 & 0 & A_1 \\ A_2 & -A_1 & 0 \end{bmatrix}$ is the matrix in the main lemma.

From the main lemma:

$$A = i \sum_j (\lambda_{j,1} |v_{j,1}\rangle\langle v_{j,1}| + \lambda_{j,2} |v_{j,2}\rangle\langle v_{j,2}| + \lambda_{j,3} |v_{j,3}\rangle\langle v_{j,3}|)$$

where $\lambda_{j,1}, \lambda_{j,2}, \lambda_{j,3}$ and $|v_{j,1}\rangle, |v_{j,2}\rangle, |v_{j,3}\rangle$ are defined in the main lemma.

Pick an orthonormal basis $\{|w_k\rangle\}$ of space $H_B \otimes H_C$. Then

$$\widetilde{A} = A \otimes I \otimes I = i \sum_{j,k} (\lambda_{j,1} |v_{j,1}\rangle\langle v_{j,1}| \otimes |w_k\rangle\langle w_k| + \lambda_{j,2} |v_{j,2}\rangle\langle v_{j,2}| \otimes |w_k\rangle\langle w_k| + \lambda_{j,3} |v_{j,3}\rangle\langle v_{j,3}| \otimes |w_k\rangle\langle w_k|)$$

and $\{|v_{j,1}\rangle \otimes |w_k\rangle, |v_{j,2}\rangle \otimes |w_k\rangle, |v_{j,3}\rangle \otimes |w_k\rangle\}$ forms an orthonormal basis of space $H_A \otimes H_B \otimes H_C$.

Suppose

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \sum_{j,k} (\alpha_{j,k,1} |v_{j,1}\rangle \otimes |w_k\rangle + \alpha_{j,k,2} |v_{j,2}\rangle \otimes |w_k\rangle + \alpha_{j,k,3} |v_{j,3}\rangle \otimes |w_k\rangle)$$

and

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \sum_{j,k} (\beta_{j,k,1} |v_{j,1}\rangle \otimes |w_k\rangle + \beta_{j,k,2} |v_{j,2}\rangle \otimes |w_k\rangle + \beta_{j,k,3} |v_{j,3}\rangle \otimes |w_k\rangle$$

Then

$$x^\dagger \widetilde{A} y = i \sum_{j,k} (\lambda_{j,1} \overline{\alpha_{j,k,1}} \beta_{j,k,1} + \lambda_{j,2} \overline{\alpha_{j,k,2}} \beta_{j,k,2} + \lambda_{j,3} \overline{\alpha_{j,k,3}} \beta_{j,k,3})$$

The goal is to bound this value by $3\sqrt{3}$. Since $x^\dagger \widetilde{A} y \in R$, we only need to bound $\Re(x^\dagger \widetilde{A} y)$
We know that

$$\sum_{j,k}(|\alpha_{j,k,1}|^2 + |\alpha_{j,k,2}|^2 + |\alpha_{j,k,3}|^2) = x^\dagger x = 3.$$

Similarly,

$$\sum_{j,k}(|\beta_{j,k,1}|^2 + |\beta_{j,k,2}|^2 + |\beta_{j,k,3}|^2) = y^\dagger y = 3$$

From the construction of $|v_{j,1}\rangle, |v_{j,2}\rangle$ and $|v_{j,3}\rangle$ in the main lemma, we see that the first n-dimensions of them are all $|u_j\rangle$. We get:

$$\begin{aligned} x_1 &= \sum_{j,k}(\alpha_{j,k,1}|u_j\rangle \otimes |w_k\rangle + \alpha_{j,k,2}|u_j\rangle \otimes |w_k\rangle + \alpha_{j,k,3}|u_j\rangle \otimes |w_k\rangle) \\ &= \sum_{j,k}(\alpha_{j,k,1} + \alpha_{j,k,2} + \alpha_{j,k,3})|u_j\rangle \otimes |w_k\rangle \end{aligned}$$

From definition $x_1 = \widetilde{B_1}|\psi\rangle = (I \otimes B_1 \otimes I)|\psi\rangle$, so

$$(I \otimes B_1 \otimes I)|\psi\rangle = \sum_{j,k}(\alpha_{j,k,1} + \alpha_{j,k,2} + \alpha_{j,k,3})|u_j\rangle \otimes |w_k\rangle$$

which implies

$$\begin{aligned} |\psi\rangle &= (I \otimes B_1 \otimes I) \sum_{j,k}(\alpha_{j,k,1} + \alpha_{j,k,2} + \alpha_{j,k,3})|u_j\rangle \otimes |w_k\rangle \\ &= \sum_{j,k}(\alpha_{j,k,1} + \alpha_{j,k,2} + \alpha_{j,k,3})|u_j\rangle \otimes [(B_1 \otimes I)|w_k\rangle] \end{aligned}$$

Similarly, from y_1 we can get

$$|\psi = \sum_{j,k}(\beta_{j,k,1} + \beta_{j,k,2} + \beta_{j,k,3})|u_j\rangle \otimes [(I \otimes C_1)|w_k\rangle]$$

Therefore,

$$\sum_{j,k}(\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3})|u_j\rangle\otimes[(B_1\otimes I)|w_k\rangle]=\sum_{j,k}(\beta_{j,k,1}+\beta_{j,k,2}+\beta_{j,k,3})|u_j\rangle\otimes[(I\otimes C_1)|w_k\rangle].$$

Since $|u_j\rangle$ are an orthonormal basis, so for each j, it must be

$$\sum_{k}(\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3})(B_1\otimes I)|w_k\rangle=\sum_{k}(\beta_{j,k,1}+\beta_{j,k,2}+\beta_{j,k,3})(I\otimes C_1)|w_k\rangle$$

or we can write

$$\sum_{k}(\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3})(B_1\otimes C_1)|w_k\rangle=\sum_{k}(\beta_{j,k,1}+\beta_{j,k,2}+\beta_{j,k,3})|w_k\rangle$$

Recall that we pick the orthonormal basis $\{|w_k\rangle\}$ of $H_B\otimes H_C$ arbitrarily, so we can assume $|w_k\rangle$ are eigenvectors of $B_1\otimes C_1$. Notice that $B_1\otimes C_1$ only have eigenvalues $\{1,-1\}$, let $\{|w_k\rangle : k\in K_+\}$ be the set of eigenvectors corresponding to +1 and $\{|w_k\rangle : k\in K_-\}$ be the set of eigenvectors corresponding to -1. Then:

$$\sum_{k\in K_+}(\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3})|w_k\rangle-\sum_{k\in K_-}(\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3})|w_k\rangle=\sum_{k}(\beta_{j,k,1}+\beta_{j,k,2}+\beta_{j,k,3})|w_k\rangle$$

Thus,

$$\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3}=\beta_{j,k,1}+\beta_{j,k,2}+\beta_{j,k,3}$$

if $k\in K+$, and:

$$\alpha_{j,k,1}+\alpha_{j,k,2}+\alpha_{j,k,3}=-(\beta_{j,k,1}+\beta_{j,k,2}+\beta_{j,k,3})$$

if $k\in K-$.
Now we can use the second lemma: Since $\lambda_{j,1},\lambda_{j,2},\lambda_{j,3}$ are the roots of $z(3-z^2)=\eta_j$:

$$\begin{aligned}&|\Re(i\lambda_{j,1}\overline{\alpha_{j,k,1}}\beta_{j,k,1}+i\lambda_{j,2}\overline{\alpha_{j,k,2}}\beta_{j,k,2}+i\lambda_{j,3}\overline{\alpha_{j,k,3}}\beta_{j,k,3})|\\ \le\ &\sqrt{3}\sqrt{|\alpha_{j,k,1}|^2+|\alpha_{j,k,2}|^2+|\alpha_{j,k,3}|^2}\cdot\sqrt{|\beta_{j,k,1}|^2+|\beta_{j,k,2}|^2+|\beta_{j,k,3}|^2}\end{aligned}$$

We know $x^\dagger Ay$ is a real number, so $x^\dagger\widetilde{A}y=\Re(x^\dagger\widetilde{A}y)$. It follows:

$$
\begin{aligned}
|x^\dagger \widetilde{A} y| = |\Re(x^\dagger \widetilde{A} y)| &= \left| \Re\left(i \sum_{j,k} (\lambda_{j,1} \overline{\alpha_{j,k,1}} \beta_{j,k,1} + \lambda_{j,2} \overline{\alpha_{j,k,2}} \beta_{j,k,2} + \lambda_{j,3} \overline{\alpha_{j,k,3}} \beta_{j,k,3}) \right) \right| \\
&\leq \sum_{j,k} |\Re(i\lambda_{j,1} \overline{\alpha_{j,k,1}} \beta_{j,k,1} + i\lambda_{j,2} \overline{\alpha_{j,k,2}} \beta_{j,k,2} + i\lambda_{j,3} \overline{\alpha_{j,k,3}} \beta_{j,k,3})| \\
&\leq \sum_{j,k} \sqrt{3} \sqrt{|\alpha_{j,k,1}|^2 + |\alpha_{j,k,2}|^2 + |\alpha_{j,k,3}|^2} \cdot \sqrt{|\beta_{j,k,1}|^2 + |\beta_{j,k,2}|^2 + |\beta_{j,k,3}|^2} \\
&\leq \sqrt{3} \sqrt{\sum_{j,k} (|\alpha_{j,k,1}|^2 + |\alpha_{j,k,2}|^2 + |\alpha_{j,k,3}|^2)} \cdot \sqrt{\sum_{j,k} (|\beta_{j,k,1}|^2 + |\beta_{j,k,2}|^2 + |\beta_{j,k,3}|^2)} \\
&= 3\sqrt{3}
\end{aligned}
$$

Proof of Corollary We label the entries of the magic square by $q_{j,k} (j, k = 1, 2, 3)$.

$$
\begin{aligned}
\omega_q(G) = \frac{1}{6} \sum_{j=1}^{3} \left(\frac{1}{6} \sum_{\sigma \in S_3} \sum_{a \oplus b \oplus c = 0} Pr(abc | q_{j,\sigma(1)} q_{j,\sigma(2)} q_{j,\sigma(3)}) \right) + \\
\frac{1}{6} \sum_{j=1}^{3} \left(\frac{1}{6} \sum_{\sigma \in S_3} \sum_{a \oplus b \oplus c = 0} Pr(abc | q_{\sigma(1),k} q_{\sigma(2),k} q_{\sigma(3),k} \right)
\end{aligned}
$$

Here we use the same notations as in [37], $Pr(abc|q_1 q_2 q_3)$ is the probability that if Alice, Bob and Charlie receive queries q_1, q_2, q_3 and answer a, b, c respectively. The first term is the probability that the verifier randomly picks a row j and ask Alice, Bob and Charlie different entries $q_{j,\sigma(1)}, q_{j,\sigma(2)}$, and $q_{j,\sigma(3)}$ respectively. The second term is the probability that the verifier randomly picks a column k and asks different entries. We can replace the probability by $|\psi\rangle$ and the observables. It is easy to check that:

$$
\sum_{a \oplus b \oplus c = 0} Pr(abc | q_{j,\sigma(1)} q_{j,\sigma(2)} q_{j,\sigma(3)}) = \frac{1}{2} (1 + \langle \psi | A_{j,\sigma(1)} \otimes B_{j,\sigma(2)} \otimes C_{j,\sigma(3)} | \psi \rangle)
$$

and

$$
\sum_{a \oplus b \oplus c = 0} Pr(abc | q_{\sigma(1),k} q_{\sigma(2),k} q_{\sigma(3),k}) = \frac{1}{2} (1 - \langle \psi | A_{\sigma(1),k} \otimes B_{\sigma(2),k} \otimes C_{\sigma(3),k} | \psi \rangle)
$$

so

$$\omega_q(G) = \frac{1}{2} + \frac{1}{72}\sum_{j=1}^{3}\left(\sum_{\sigma\in S_3}\langle\psi|A_{j,\sigma(1)}\otimes B_{j,\sigma(2)}\otimes C_{j,\sigma(3)}|\psi\rangle\right) - \frac{1}{72}\sum_{j=1}^{3}\left(\sum_{\sigma\in S_3}\langle\psi|A_{\sigma(1),k}\otimes B_{\sigma(2),k}\otimes C_{\sigma(3),k}|\psi\rangle\right)$$

To prove that $\omega_q(G) \leq \frac{1}{4}(2+\sqrt{3})$ we only need to show

$$\sum_{j=1}^{3}\sum_{\sigma\in S_3}\left(\langle\psi|A_{j,\sigma(1)}\otimes B_{j,\sigma(2)}\otimes C_{j,\sigma(3)}|\psi\rangle - \langle\psi|A_{\sigma(1),j}\otimes B_{\sigma(2),j}\otimes C_{\sigma(3),j}|\psi\rangle\right) \leq 18\sqrt{3}$$

Or

$$\sum_{j=1}^{3}\sum_{\sigma\in S_3}\left(\langle A_{j,\sigma(1)}\otimes B_{j,\sigma(2)}\otimes C_{j,\sigma(3)} - A_{\sigma(1),j}\otimes B_{\sigma(2),j}\otimes C_{\sigma(3),j}\rangle\right) \leq 18\sqrt{3}$$

Denote the the left side of the above equation by L. We will compute L in a different order,

$$\begin{aligned} L &= \sum_{\sigma\in S_3}\sum_{j=1}^{3}\left(\langle A_{j,\sigma(1)}\otimes B_{j,\sigma(2)}\otimes C_{j,\sigma(3)} - A_{\sigma(1),j}\otimes B_{\sigma(2),j}\otimes C_{\sigma(3),j}\rangle\right) \\ &\leq \sum_{\sigma\in S_3}\left|\sum_{j=1}^{3}\langle A_{j,\sigma(1)}\otimes B_{j,\sigma(2)}\otimes C_{j,\sigma(3)} - A_{\sigma(1),j}\otimes B_{\sigma(2),j}\otimes C_{\sigma(3),j}\rangle\right| \end{aligned}$$

By the main theorem we know that for any $\sigma \in S_3$,

$$\left|\sum_{j=1}^{3}\langle A_{j,\sigma(1)}\otimes B_{j,\sigma(2)}\otimes C_{j,\sigma(3)} - A_{\sigma(1),j}\otimes B_{\sigma(2),j}\otimes C_{\sigma(3),j}\rangle\right| \leq 3\sqrt{3}$$

thus $L \leq 6\times 3\sqrt{3} = 18\sqrt{3}$.

2.4 Proof of Theorem 2.2.3

We can represent $\omega_{ns}(G)$ as the maximum value of a linear programming problem. The conditional probabilities are the variables and the no-signaling conditions/normalization properties give constraints on the linear program.

First we need to decide how many variables we have in this linear program. There are several symmetries in Magic Square game we can use:

1. Symmetries between Alice, Bob and Charlie: if we permute the roles of Alice, Bob and Charlie, and also permute their answers, then the probability remains the same, i.e.

$$Pr(A_1A_2A_3|q_{j_1,k_1}, q_{j_2,k_2}, q_{j_3,k_3}) = Pr(a_{\sigma(1)}a_{\sigma(2)}a_{\sigma(3)}|q_{j_{\sigma(1)},k_{\sigma(1)}}, q_{j_{\sigma(2)},k_{\sigma(2)}}, q_{j_{\sigma(3)},k_{\sigma(3)}})(\forall\sigma \in S_3)$$

2. Symmetries between the three rows: The probability are the same if we permutate the rows in the query part, i.e.

$$Pr(a, b, c|q_{j_1,k_1}, q_{j_2,k_2}, q_{j_3,k_3}) = Pr(a, b, c|q_{\sigma(j_1),k_1}, q_{\sigma(j_2),k_2}, q_{\sigma(j_3),k_3})(\forall\sigma \in S_3)$$

3. Symmetries between the three columns:

$$Pr(a, b, c|q_{j_1,k_1}, q_{j_2,k_2}, q_{j_3,k_3}) = Pr(a, b, c|q_{j_1,\sigma(k_1)}, q_{j_2,\sigma(k_2)}, q_{j_3,\sigma(k_3)})(\forall\sigma \in S_3)$$

4. Skew symmetries between row and columns:

$$Pr(a_1a_2a_3|q_{j_1,k_1}q_{j_2,k_2}q_{j3,k3}) = Pr(a_1a_2a_3|q_{k_1,j_1}q_{k_2,j_2}q_{k_3,j_3})$$

Using 1 through 4 to reduce the number of independent variables, we have finally the following variables:

$$Pr(000|q_{1,1}q_{1,1}q_{1,1}) = x_0, Pr(001|q_{1,1}q_{1,1}q_{1,1}) = x_1$$

$$Pr(000|q_{1,1}q_{1,1}q_{1,2}) = y_0, Pr(001|q_{1,1}q_{1,1}q_{2,1}) = y_1, Pr(010|q_{1,1}q_{1,1}q_{1,2}) = y_2, Pr(011|q_{1,1}q_{1,1}q_{1,2}) = y_3$$

$$Pr(000|q_{1,1}q_{1,2}q_{1,3}) = z_0, Pr(001|q_{1,1}q_{1,2}q_{1,3}) = z_1, Pr(011|q_{1,1}q_{1,2}q_{1,3}) = z_3, Pr(111|q_{1,1}q_{1,2}q_{1,3}) = z_7$$

$$Pr(000|q_{1,1}q_{1,1}q_{2,2}) = u_0, Pr(001|q_{1,1}q_{1,1}q_{2,2}) = u_1, Pr(010|q_{1,1}q_{1,1}q_{2,2}) = u_2$$

$$Pr(000|q_{1,1}q_{1,2}q_{2,1}) = v_0, Pr(001|q_{1,1}q_{1,2}q_{2,1}) = v_1, Pr(010|q_{1,1}q_{1,2}q_{2,1}) = v_2, Pr(011|q_{1,1}q_{1,2}q_{2,1}) = v_3$$

$$Pr(000|q_{1,1}q_{1,2}q_{2,3}) = w_0, Pr(001|q_{1,1}q_{1,2}q_{2,3}) = w_1, Pr(010|q_{1,1}q_{1,2}q_{2,3}) = w_2$$
$$Pr(011|q_{1,1}q_{1,2}q_{2,3}) = w_3, Pr(110|q_{1,1}q_{1,2}q_{2,3}) = w_6, Pr(111|q_{1,1}q_{1,2}q_{2,3}) = w_7$$

$Pr(000|q_{1,1}q_{2,2}q_{3,3}) = r_0, Pr(001|q_{1,1}q_{2,2}q_{3,3}) = r_1, Pr(010|q_{1,1}q_{2,2}q_{3,3}) = r_2, Pr(011|q_{1,1}q_{2,2}q_{3,3}) = r_3$

The objective function is

$$\frac{1}{6} \cdot 3[Pr(000|q_{1,1}q_{1,2}q_{1,3}) + 3Pr(011|q_{1,1}q_{1,2}q_{1,3})] + \frac{1}{6} \cdot 3[Pr(111|q_{1,1}q_{2,1}q_{3,1}) + 3Pr(001|q_{1,1}q_{2,1}q_{3,1})]$$
$$= Pr(000|q_{1,1}q_{1,2}q_{1,3}) + 3Pr(011|q_{1,1}q_{1,2}q_{1,3}) = z_0 + 3z_3$$

The linear programming is easy to solve: when $x_0 = 0.5, x_1 = 0, y_0 = y_1 = y_6 = y_7 = 0.25, y_2 = y_3 = 0, z_0 = z_3 = 0.25, z_1 = z_7 = 0, u_0 = u_1 = 0.25, u_2 = 0, v_0 = v_1 = v_2 = v_3 = 0.125, w_0 = w_3 = w_6 = 0.25, w_1 = w_2 = w_7 = 0$, and $r_0 = r_1 = 0.125$, it has optimal value $\omega_{ns}(G) = 1$.

2.5 Proof of Theorem 2.2.4

We define some notations first: H_A, H_B and H_C are the subspace of Alice, Bob and Charlie. A_j, B_j and C_j are the observables corresponding to Alice, Bob and Charlie's measurement if they receive a query x_j, $j = 1, ..., n$. For any $s_1, s_2, s_3 \in \{-1, +1\}$, define a subspace

$$H_{A,jkl}^{s_1 s_2 s_3} = \{|\phi\rangle \in H_A : A_j|\phi\rangle = s_1|\phi\rangle, A_k|\phi\rangle = s_2|\phi\rangle, A_l|\phi\rangle = s_3|\phi\rangle\}$$

Similarly we can define $H_{B,jkl}^{s_1 s_2 s_3}$ and $H_{B,jkl}^{s_1 s_2 s_3}$. We will write $H_{A,jkl}^{+1+1+1}$ as $H_{A,jkl}^{+++}$ for short, similarly for other subspace. It is clear that if $(s_1 s_2 s_3) \neq (s_1' s_2' s_3')$, then $H_{A,jkl}^{s_1 s_2 s_3}$ and $H_{A,jkl}^{s_1' s_2' s_3'}$ are orthogonal for any j, k, l.

We now proceed to prove the main theorem. If $\omega_c(G) = 1$, it is clear that $\omega_q(G) = 1$. So we only need to give proof for the other direction.

We first consider the case when f only has one clause. Without loss of generality we can assume $f = x_1 \vee x_2 \vee x_3$, then

$$\omega_q(f) = \frac{1}{6}\sum_{j=1}^{3}(Pr(000|jjj) + Pr(111|jjj)) + \frac{1}{12}\sum_{\{j,k,l\}=\{1,2,3\}}(1 - Pr(000|jkl))$$

The first term above is the probability when Alice, Bob and Charlie were asked the same query and answer the same value, the second term is that they were asked different variables.

We can rewrite $Pr(abc|q_1q_2q_3)$ by using $|\psi\rangle$ and the observables A_j, B_k, C_l ,

$$\omega_q(f) = \frac{1}{6}\sum_{j=1}^{3}\left(\langle\psi|\frac{I+A_j}{2}\otimes\frac{I+B_j}{2}\otimes\frac{I+C_j}{2}|\psi\rangle + \langle\psi|\frac{I-A_j}{2}\otimes\frac{I-B_j}{2}\otimes\frac{I-C_j}{2}|\psi\rangle\right)$$
$$+\frac{1}{12}\sum_{\{j,k,l\}=\{1,2,3\}}\left(1-\langle\psi|\frac{I+A_j}{2}\otimes\frac{I+B_k}{2}\otimes\frac{I+C_l}{2}|\psi\rangle\right)$$
$$= \frac{1}{24}\sum_{j=1}^{3}(1+\langle\psi|A_j\otimes B_j\otimes I|\psi\rangle + \langle\psi|A_j\otimes I\otimes C_j|\psi\rangle + \langle\psi|I\otimes B_j\otimes C_j|\psi\rangle)$$
$$+\frac{1}{24}\sum_{\{j,k,l\}=\{1,2,3\}}\left(1-\langle\psi|\frac{I+A_j}{2}\otimes\frac{I+B_k}{2}\otimes\frac{I+C_l}{2}|\psi\rangle\right)$$

So, if $\omega_q(f)=1$ the the following conditions apply: for all j, $\langle\psi|A_j\otimes B_j\otimes I|\psi\rangle = 1$, $\langle\psi|A_j\otimes I\otimes C_j|\psi\rangle = 1$, $\langle\psi|I\otimes B_j\otimes C_j|\psi\rangle = 1$, and for all $\{j,k,l\}=\{1,2,3\}$, $\langle\psi|\frac{1+A_j}{2}\otimes\frac{1+B_k}{2}\otimes\frac{1+C_l}{2}|\psi\rangle = 0$.

Lemma 2.5.1. *For all j, $\langle\psi|A_j\otimes B_j\otimes I|\psi\rangle = 1$, $\langle\psi|A_j\otimes I\otimes C_j|\psi\rangle = 1$, $\langle\psi|I\otimes B_j\otimes C_j|\psi\rangle = 1$, if and only if $|\psi\rangle = \sum_{s_1s_2s_3\in\{+,-\}}|\psi_{s_1s_2s_3}\rangle$, where $|\psi_{s_1s_2s_3}\rangle \in H_{A,j_1j_2j_3}^{s_1s_2s_3}\otimes H_{B,j_1j_2j_3}^{s_1s_2s_3}\otimes H_{C,j_1j_2j_3}^{s_1s_2s_3}$*

Proof. To simplify notations, we assume $\{j_1,j_2,j_3\}=\{1,2,3\}$. One directiondirection is easy to check. We only focus on the other direction. Since $H_B = H_{B,1}^{+}\oplus H_{B,1}^{-}, H_C = H_{C,2}^{+}\oplus H_{C,2}^{-}$, so $H_B\otimes H_C = (H_{B,1}\otimes H_{C,2})\oplus(H_{B,1}\otimes H_{C,2})\oplus(H_{B,1}\otimes H_{C,2})\oplus(H_{B,1}\otimes H_{C,2})$. Suppose $|\psi\rangle = |\psi_{++}\rangle + |\psi_{+-}\rangle + |\psi_{-+}\rangle + |\psi_{--}\rangle$ is the orthogonal decomposition of $|\psi\rangle$, where

$$|\psi_{++}\rangle \in H_A\otimes H_{B,1}^{+}\otimes H_{C,2}^{+}$$
$$|\psi_{+-}\rangle \in H_A\otimes H_{B,1}^{+}\otimes H_{C,2}^{-}$$
$$|\psi_{-+}\rangle \in H_A\otimes H_{B,1}^{-}\otimes H_{C,2}^{+}$$
$$|\psi_{--}\rangle \in H_A\otimes H_{B,1}^{-}\otimes H_{C,2}^{-}$$

Since $\langle\psi|A_1\otimes B_1\otimes I|\psi\rangle = 1$, it follows that $\widetilde{A_1}|\psi\rangle = \widetilde{B_1}|\psi\rangle$. Here the notation $\widetilde{A_1},\widetilde{B_1}$ are similar as in the previous sections. Thus

$$\widetilde{A_1}|\psi_{++}\rangle + \widetilde{A_1}|\psi_{+-}\rangle + \widetilde{A_1}|\psi_{-+}\rangle + \widetilde{A_1}|\psi_{--}\rangle = |\psi_{++}\rangle + |\psi_{+-}\rangle - |\psi_{-+}\rangle - |\psi_{--}\rangle$$

We know that $H_A\otimes H_{B,1}^{+}\otimes H_{C,2}^{+}$, $H_A\otimes H_{B,1}^{+}\otimes H_{C,2}^{-}$, $H_A\otimes H_{B,1}^{-}\otimes H_{C,2}^{+}$, $H_A\otimes H_{B,1}^{-}\otimes H_{C,2}^{-}$ is an orthogonal decomposition of the whole space, and operator $\widetilde{A_1}$ will not apply to space H_B and H_C, so the only way is that:

$$\widetilde{A_1}|\psi_{++}\rangle = |\psi_{++}\rangle, \widetilde{A_1}|\psi_{+-}\rangle = |\psi_{+-}\rangle, \widetilde{A_1}|\psi_{-+}\rangle = -|\psi_{-+}\rangle, \widetilde{A_1}|\psi_{--}\rangle = -|\psi_{--}\rangle$$

Therefore,

$$|\psi_{++}\rangle \in H^{+}_{A,1} \otimes H^{+}_{B,1} \otimes H^{+}_{C,2}$$
$$|\psi_{+-}\rangle \in H^{+}_{A,1} \otimes H^{+}_{B,1} \otimes H^{-}_{C,2}$$
$$|\psi_{-+}\rangle \in H^{-}_{A,1} \otimes H^{-}_{B,1} \otimes H^{+}_{C,2}$$
$$|\psi_{--}\rangle \in H^{-}_{A,1} \otimes H^{-}_{B,1} \otimes H^{-}_{C,2}$$

Similarly, from $\langle\psi|A_2 \otimes I \otimes C_2|\psi\rangle = 1$, we can get:

$$\widetilde{A_2}|\psi_{++}\rangle = |\psi_{++}\rangle, \widetilde{A_2}|\psi_{+-}\rangle = -|\psi_{+-}\rangle, \widetilde{A_2}|\psi_{-+}\rangle = |\psi_{-+}\rangle, \widetilde{A_2}|\psi_{--}\rangle = -|\psi_{--}\rangle$$

Thus,

$$|\psi_{++}\rangle \in H^{+}_{A,2} \otimes H^{+}_{B,1} \otimes H^{+}_{C,2}$$
$$|\psi_{+-}\rangle \in H^{-}_{A,2} \otimes H^{+}_{B,1} \otimes H^{-}_{C,2}$$
$$|\psi_{-+}\rangle \in H^{+}_{A,2} \otimes H^{-}_{B,1} \otimes H^{+}_{C,2}$$
$$|\psi_{--}\rangle \in H^{-}_{A,2} \otimes H^{-}_{B,1} \otimes H^{-}_{C,2}$$

Combining the last two sets of equations, we have:

$$|\psi_{++}\rangle \in H^{++}_{A,12} \otimes H^{+}_{B,1} \otimes H^{+}_{C,2}$$
$$|\psi_{+-}\rangle \in H^{+-}_{A,12} \otimes H^{+}_{B,1} \otimes H^{-}_{C,2}$$
$$|\psi_{-+}\rangle \in H^{-+}_{A,12} \otimes H^{-}_{B,1} \otimes H^{+}_{C,2}$$
$$|\psi_{--}\rangle \in H^{--}_{A,12} \otimes H^{-}_{B,1} \otimes H^{-}_{C,2}$$

If we further consider $\langle\psi|A_1 \otimes I \otimes C_1|\psi\rangle = 1$ and $\langle\psi|A_2 \otimes B_2 \otimes I|\psi\rangle = 1$, we can prove that

$$|\psi_{++}\rangle \in H^{++}_{A,12} \otimes H^{++}_{B,12} \otimes H^{++}_{C,12}$$
$$|\psi_{+-}\rangle \in H^{+-}_{A,12} \otimes H^{+-}_{B,12} \otimes H^{+-}_{C,12}$$
$$|\psi_{-+}\rangle \in H^{-+}_{A,12} \otimes H^{-+}_{B,12} \otimes H^{-+}_{C,12}$$
$$|\psi_{--}\rangle \in H^{--}_{A,12} \otimes H^{--}_{B,12} \otimes H^{--}_{C,12}$$

Now we consider A_3, B_3 and C_3 , from $\langle\psi|A_3 \otimes B_3 \otimes I|\psi\rangle = 1$ we have:

$$\widetilde{A_3}|\psi_{++}\rangle + \widetilde{A_3}|\psi_{+-}\rangle + \widetilde{A_3}|\psi_{-+}\rangle + \widetilde{A_3}|\psi_{--}\rangle = \widetilde{B_3}|\psi_{++}\rangle + \widetilde{B_3}|\psi_{+-}\rangle + \widetilde{B_3}|\psi_{-+}\rangle + \widetilde{B_3}|\psi_{--}\rangle$$

Consider the above equation in space H_C. Operators A_3, B_3 do not apply in H_C , so $\widetilde{A_3}|\psi_{s_1s_2}\rangle$, $\widetilde{B_3}|\psi_{s_1s_2}\rangle \in H_A \otimes H_B \otimes H_{C,12}^{s_1s_2}$ for any $s_1, s_2 \in \{-,+\}$. But $H_{C,12}^{++}, H_{C,12}^{+-}, H_{C,12}^{-+}, H_{C,12}^{--}$ are orthogonal subspaces of H_C, so

$$\widetilde{A_3}|\psi_{++}\rangle = \widetilde{B_3}|\psi_{++}\rangle, \widetilde{A_3}|\psi_{+-}\rangle = \widetilde{B_3}|\psi_{+-}\rangle, \widetilde{A_3}|\psi_{-+}\rangle = \widetilde{B_3}|\psi_{-+}\rangle, \widetilde{A_3}|\psi_{--}\rangle = \widetilde{B_3}|\psi_{--}\rangle$$

Similarly,

$$\widetilde{A_3}|\psi_{++}\rangle = \widetilde{C_3}|\psi_{++}\rangle, \widetilde{A_3}|\psi_{+-}\rangle = \widetilde{C_3}|\psi_{+-}\rangle, \widetilde{A_3}|\psi_{-+}\rangle = \widetilde{C_3}|\psi_{-+}\rangle, \widetilde{A_3}|\psi_{--}\rangle = \widetilde{C_3}|\psi_{--}\rangle$$

Therefore,

$$\widetilde{A_j}|\psi_{s_1s_2} = \widetilde{B_j}|\psi_{s_1s_2} = \widetilde{C_j}|\psi_{s_1s_2}, \forall s_1, s_2 \in \{-,+\}, j = 1,2,3$$

We know that $|\psi_{++}\rangle \in H_{A,1}^{+} \otimes H_{B,2}^{+} \otimes I$, and $H_C = H_{C,3}^{+} \oplus H_{C,3}^{-}$, so we can decompose $|\psi_{++}\rangle$ on it: $|\psi_{++}\rangle = |\psi_{+++}\rangle + |\psi_{++-}\rangle$, where

$$|\psi_{+++}\rangle \in H_{A,1}^{+} \otimes H_{B,2}^{+} \otimes H_{C,3}^{+}, |\psi_{++-}\rangle \in H_{A,1}^{+} \otimes H_{B,2}^{+} \otimes H_{C,3}^{-}$$

It follwos that:

$$|\psi_{+++}\rangle \in H_{A,123}^{+++} \otimes H_{B,123}^{+++} \otimes H_{C,123}^{+++}, |\psi_{++-}\rangle \in H_{A,123}^{++-} \otimes H_{B,123}^{++-} \otimes H_{C,123}^{++-}$$

Similarly we can decompose $|\psi_{+-}\rangle, |\psi_{-+}\rangle, |\psi_{--}\rangle$ and prove the corresponding properties.

□

From the previous lemma we know that

$$|\psi\rangle \in \bigoplus_{s_1s_2s_3 \in \{+,-\}} H_{A,123}^{s_1s_2s_3} \otimes H_{B,123}^{s_1s_2s_3} \otimes H_{C,123}^{s_1s_2s_3}$$

and also

$$\langle\psi|\frac{1+A_1}{2} \otimes \frac{1+B_2}{2} \otimes \frac{1+C_3}{2}|\psi\rangle = 0$$

Setting $|\psi\rangle = \sum_{s_1 s_2 s_3} |\psi_{s_1 s_2 s_3}\rangle$ in this equation, and using the fact that $\sum_{s_1 s_2 s_3} |||\psi_{s_1 s_2 s_3}\rangle||^2 = \langle\psi|\psi\rangle = 1$ to simplify it, we get:

$$|||\psi_{+++}\rangle|| = 0, |\psi_{+++}\rangle = 0$$

Thus $|\psi\rangle$ is the superposition of a classical assignment, i.e.

$$|\psi\rangle \in \bigoplus_{s_1 s_2 s_3 \in \{+,-\}, (s_2 s_2 s_3) \neq (+++)} H_{A,123}^{s_1 s_2 s_3} \otimes H_{B,123}^{s_1 s_2 s_3} \otimes H_{C,123}^{s_1 s_2 s_3}$$

Suppose $f = f_1 \wedge f_2 \wedge ... \wedge f_m$, $f_i = X_{j_i} \vee X_{k_i} \vee X_{l_i}$ are clauses ($i = 1, ..., m$), literal $X_h = x_h$ or $X_h = \overline{x_h}$, ($h = 1, ..., n$). Then

$$\omega_q(f) = \frac{1}{6m} \sum_{i=1}^{m} [(Pr(000|j_i j_i j_i) + Pr(111|j_i j_i j_i)) +$$
$$(Pr(000|k_i k_i k_i) + Pr(111|k_i k_i k_i)) + (Pr(000|l_i l_i l_i) + Pr(111|l_i l_i l_i))]$$
$$+ \frac{1}{12m} \sum_{i=1}^{m} \left[\sum_{\{j,k,l\} = \{j_i, k_i, l_i\}} \Big(1 - Pr(X_j X_k X_l = 000|jkl)\Big) \right]$$

$\omega_q(f) = 1$ implies that for $i = 1...m$ and $\{j, k, l\} = \{j_i, k_i, l_i\}$:

$$Pr(000|j_i j_i j_i) + Pr(111|j_i j_i j_i) = 1$$
$$Pr(000|k_i k_i k_i) + Pr(111|k_i k_i k_i) = 1$$
$$Pr(000|l_i l_i l_i) + Pr(111|l_i l_i l_i) = 1$$
$$Pr(X_j X_k X_l = 000|jkl) = 0$$

Similarly we can rewrite the probability using $|\psi\rangle$ and the observables; we have for all $i = 1...m$:

$$1 + \langle\psi|A_{j_i} \otimes B_{j_i} \otimes I|\psi\rangle + \langle\psi|A_{j_i} \otimes I \otimes C_{j_i}|\psi\rangle + \langle\psi|I \otimes B_{j_i} \otimes C_{j_i}|\psi\rangle = 4$$
$$1 + \langle\psi|A_{k_i} \otimes B_{k_i} \otimes I|\psi\rangle + \langle\psi|A_{k_i} \otimes I \otimes C_{k_i}|\psi\rangle + \langle\psi|I \otimes B_{k_i} \otimes C_{k_i}|\psi\rangle = 4$$
$$1 + \langle\psi|A_{l_i} \otimes B_{l_i} \otimes I|\psi\rangle + \langle\psi|A_{l_i} \otimes I \otimes C_{l_i}|\psi\rangle + \langle\psi|I \otimes B_{l_i} \otimes C_{l_i}|\psi\rangle = 4$$

i.e. for $i = 1...m$:

$$\widetilde{A_{j_i}}|\psi\rangle = \widetilde{B_{j_i}}|\psi\rangle = \widetilde{C_{j_i}}|\psi\rangle$$
$$\widetilde{A_{k_i}}|\psi\rangle = \widetilde{B_{k_i}}|\psi\rangle = \widetilde{C_{k_i}}|\psi\rangle$$
$$\widetilde{A_{l_i}}|\psi\rangle = \widetilde{B_{l_i}}|\psi\rangle = \widetilde{C_{l_i}}|\psi\rangle$$

From the last equation we get, for all $1 \leq i \leq m$:

$$\langle\psi|(I + t_{i,1}A_{j_i}) \otimes (I + t_{i,2}B_{k_i}) \otimes (I + t_{i,3}C_{l_i})|\psi\rangle = 0$$

where $t_{i,1}, t_{i,2}$ and $t_{i,3}$ are the sign of literal X_{j_i}, X_{k_i} and X_{l_i}
Consider $i = 1, f_1 = x_{j_1} \vee X_{k_1}$. We have:

$$|\psi\rangle = \sum_{s_1s_2s_3 \in \{-,+\}, (s_1s_2s_3) \neq (t_{1,1}t_{1,2}t_{1,3})} |\psi_{s_1s_2s_3}\rangle$$

where $|\psi_{s_1s_2s_3} \in H_{A,j_1k_1l_1}^{s_1s_2s_3} \otimes H_{B,j_1k_1l_1}^{s_1s_2s_3} \otimes H_{A,j_1k_1l_1}^{s_1s_2s_3}$ Since $|||\psi\rangle||^2 = 1$, at least one of the vectors $\{|\psi_{s_1s_2s_3} : s_1, s_2, s_3 \in \{-,+\}, (s_1s_2s_3) \neq (t_{1,1}t_{1,2}t_{1,3})\}$ is nonzero. For example assume $|\psi_{s_1^*s_2^*s_3^*}\rangle \neq 0$. We claim that instead of $|\psi\rangle$, $|\psi_{s_1^*s_2^*s_3^*}\rangle$ also satisfies all the equations above (actually we will prove all $|\psi_{s_1s_2s_3}\rangle$ satisfy those equations)
(*) For any $1 \leq h \leq n$, suppose $\widetilde{A_h}|\psi\rangle = \widetilde{B_h}|\psi\rangle = \widetilde{C_h}|\psi\rangle$, then from $\widetilde{A_h}|\psi\rangle = \widetilde{B_h}|\psi\rangle$ we know

$$\widetilde{A_h} \sum_{s_1s_2s_3 \in \{-,+\}, (s_1s_2s_3) \neq (t_{1,1}t_{1,2}t_{1,3})} |\psi_{s_1s_2s_3}\rangle = \widetilde{B_h} \sum_{s_1s_2s_3 \in \{-,+\}, (s_1s_2s_3) \neq (t_{1,1}t_{1,2}t_{1,3})} |\psi_{s_1s_2s_3}\rangle$$

Consider this equation in space H_C: all $H_{C,j_1k_1l_1}^{s_1s_2s_3}$ are orthogonal subspaces of H_C and the operators $\widetilde{A_h}$ and $\widetilde{B_h}$ do not apply to space H_C , thus $\widetilde{A_h}|\psi_{s_1s_2s_3}\rangle = \widetilde{B_h}|\psi_{s_1s_2s_3}\rangle$. Similarly, $\widetilde{A_h}|\psi_{s_1s_2s_3}\rangle = \widetilde{C_h}|\psi_{s_1s_2s_3}\rangle$. Therefore:

$$\widetilde{A_h}|\psi_{s_1s_2s_3}\rangle = \widetilde{B_h}|\psi_{s_1s_2s_3}\rangle = \widetilde{C_h}|\psi_{s_1s_2s_3}\rangle$$

(**) We know that

$$\langle\psi|(\widetilde{I} + t_{i,1}\widetilde{A_{j_i}})(\widetilde{I} + t_{i,2}\widetilde{B_{k_i}})(\widetilde{I} + t_{i,3}\widetilde{C_{l_i}})|\psi\rangle = 0$$

We also know that $\widetilde{C_{l_i}}|\psi\rangle = \widetilde{A_{l_i}}|\psi\rangle$, which implies $(\widetilde{I} + \widetilde{C_{l_i}})|\psi\rangle = (\widetilde{I} + \widetilde{A_{l_i}})|\psi\rangle$. Thus, we can replace operator C_{l_i} by A_{l_i}:

$$\langle\psi|(\widetilde{I} + t_{i,1}\widetilde{A_{j_i}})(\widetilde{I} + t_{i,2}\widetilde{B_{k_i}})(\widetilde{I} + t_{i,3}\widetilde{A_{l_i}})|\psi\rangle = 0$$

Now we replace $|\psi\rangle$ by $\sum_{s_1s_2s_3} |\psi_{s_1s_2s_3}\rangle$ and consider the equations in the space of H_C , and we get:

$$\langle\psi_{s_1s_2s_3}|(\widetilde{I}+t_{i,1}\widetilde{A_{j_i}})(\widetilde{I}+t_{i,2}\widetilde{B_{k_i}})(\widetilde{I}+t_{i,3}\widetilde{A_{l_i}})|\psi_{s_1s_2s_3}\rangle = 0$$

From (*) we already know that $\widetilde{A_{l_i}}|\psi_{s_1s_2s_3}\rangle = \widetilde{C_{l_i}}|\psi_{s_1s_2s_3}\rangle$, so we can replace C_{l_i} back:

$$\langle\psi_{s_1s_2s_3}|(\widetilde{I}+t_{i,1}\widetilde{A_{j_i}})(\widetilde{I}+t_{i,2}\widetilde{B_{k_i}})(\widetilde{I}+t_{i,3}\widetilde{C_{l_i}})|\psi_{s_1s_2s_3}\rangle = 0$$

From (*) and (**), $|\psi_{s_1s_2s_3}\rangle$ (and in particular, $|\psi_{s_1^*s_2^*s_3^*}\rangle$) satisfy all the original equations.
By the definition of $|\psi_{s_1s_2s_3}\rangle$:

$$\widetilde{A_{j_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = \widetilde{B_{j_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = \widetilde{C_{j_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = s_1^*|\psi_{s_1^*s_2^*s_3^*}\rangle$$
$$\widetilde{A_{k_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = \widetilde{B_{k_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = \widetilde{C_{k_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = s_2^*|\psi_{s_1^*s_2^*s_3^*}\rangle$$
$$\widetilde{A_{l_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = \widetilde{B_{l_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = \widetilde{C_{l_1}}|\psi_{s_1^*s_2^*s_3^*}\rangle = s_3^*|\psi_{s_1^*s_2^*s_3^*}\rangle$$

So $|\psi_{s_1^*s_2^*s_3^*}\rangle$ can be considered as a classical assignment of variables in f_1: $x_{j_1} = 1$ if $s_1^* = -$ and 0 if $s_1^* = +$. Similarly for x_{k_1} and x_{l_1} (with s_2^* and s_3^* respectively)

Let f' be the new formula if we put this assignment of x_{j_1}, x_{k_1} and x_{l_1} in formula f . Then f' has at most $(m-1)$ clauses and $(n-3)$ variables. We can repeat the arguments we have done for formula f. After at most $(m-1)$ rounds we will get a truth assignment for f . So $\omega_c(f) = 1$

Chapter 3

Commuting Provers

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 chapter 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, in this chapter we prove 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 $1 - 2^{-\mathrm{poly}}$.

3.1 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* [13], 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* [6]. 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 whether or not dishonest 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.

3.1.1 Our contribution

The main contribution of this work is to develop new methods 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 study uses "player" and "prover" interchangeably). Specifically, we consider *commuting-operator provers*, the notion of which was already introduced in the seminal paper by Tsirelson [40] in 1980. 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 commutativity of operators, we obtain a number of intriguing results on the limits of nonlocal strategies.

A family of n-party Tsirelson inequalities and n-player Magic Square games 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. In particular, for $n = 2$, our inequality is identical to the Tsirelson bound for the CHSH inequality. The case for $n = 3$ was originally proved with a different proof in a preliminary work by a subset of the authors (Sun, Yao and Preda [35]).

Our inequalities include the inequalities proved by Wehner [44] as special cases — our proof is completely different from hers. It is stressed that our inequalities are tight even in the usual nonlocal model with prior entanglement, a simple proof of which is also given in this study.

Our inequalities can be interpreted as the upper bound on the winning probability for commuting-operator players in an n-player cooperative game which is closely related to the Magic Square game. We call this n-player game *n-player Magic Square game*. In particular, we show that commuting-operator players cannot win with certainty in the three-player Magic Square game.

A conceptual consequence of this is that the "breakage" of the oracularization paradigm for the Magic Square game shown in Ref. [13] does not arise from allowing prior entanglement among provers alone, but arises from both allowing prior entanglement and the process of oracularization.

Three-prover one-round interactive proof systems for NP **and** NEXP 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 [19]. Because of the commutativity of operators which each prover applies, it is quite easy to apply the technique developed by Kempe, Kobayashi, Matsumoto, Toner, and Vidick [25] 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. [25] 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 [13] 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 $1 - 2^{-\mathrm{poly}}$, whereas only languages in EXP have such proof systems in the two-prover one-round binary case.

As is pointed in Ref. [13], an important consequence of Tsirelson's theorem [40] 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. Our result shows that this is not the case if we consider three players and we drop the XOR condition of the game unless P = NP.

3.1.2 Background and related work

Multi-prover interactive proof systems (MIPs) were proposed by Ben-Or, Goldwasser, Kilian and Wigderson [6]. It was proved by Babai, Fortnow and Lund [3] 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 [17]. One of the main tools when proving these claims is the *oracularization* [6, 18], which forces provers to act just like fixed proof strings.

Cleve, Høyer, Toner and Watrous [13] 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 an-

swers, recognize NEXP without prior entanglement but at most EXP with prior entanglement.

Kobayashi and Matsumoto [28] 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. Recently, Kempe, Kobayashi, Matsumoto, Toner and Vidick [25] showed that NP $\subseteq$ $\mathrm{MIP}^*_{1,1-1/\mathrm{poly}}(3,1)$ and NEXP $\subseteq$ $\mathrm{MIP}^*_{1,1-2^{-\mathrm{poly}}}(3,1)$. Subsequently to the present work, Ito, Kobayashi, and Matsumoto [22] showed that the same holds with two provers. Cleve, Gavinsky and Jain [12] proved that NP $\subseteq$ $\oplus\mathrm{MIP}^*_{1-\varepsilon,1/2+\varepsilon}(2,1)$, where $\oplus\mathrm{MIP}^*_{c(n),s(n)}(2,1)$ is the class of languages recognized by a two-prover one-round XOR interactive proof system with entangled provers.

The notion of commuting-operator provers is also used by Navascués, Pironio, and Acín [31] and Doherty, Liang, Toner, and Wehner [14] to obtain an upper bound of the entangled value of two-prover games. 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 [40, 41].

3.1.3 Organization of the chapter

Section 3.2 gives definitions on MIP systems used in later sections. Section 3.3 introduces the commuting-operator-provers model which we will use later and states some basic facts on it. Section 3.4 discusses the n-player generalization of Tsirelson's bound based on the $n\times n$ Magic Square game. Section 3.5 treats the three-prover one-round binary interactive proof system for NEXP and compares it with the two-prover case.

3.2 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 [32]) and on computational complexity (e.g. Du and Ko [15]).

The *trace distance* between two quantum states ρ and σ is defined by $D(\rho,\sigma) = (1/2)\|\rho-\sigma\|_1$, where $\|\cdot\|_1$ denotes the induced 1-norm.

See Nielsen and Chuang [32] for the proof of the following basic facts about the trace distance. Applying the same operation to two states does not increase the trace distance between them: $D(\Phi(\rho),\Phi(\sigma)) \le D(\rho,\sigma)$ for any admissible superoperator Φ. For pure states $|\varphi\rangle$ and $|\psi\rangle$, the trace distance and the inner product are related by: $D(|\varphi\rangle\langle\varphi|,|\psi\rangle\langle\psi|)^2 = 1-|\langle\varphi|\psi\rangle|^2$.

3.2.1 Games and multi-prover interactive proof systems

Here we review basic notions of multi-prover interactive proof systems that are necessary to define commuting-operator model in Section 3.3.

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*) is a pair $G = (\pi, V)$ of a probability distribution π over Q^m and a predicate $V\colon Q^m \times A^m \to \{0,1\}$, where Q and A are finite sets. As a convention, we denote $V(q_1, \ldots, q_m, a_1, \ldots, a_m)$ by $V(a_1, \ldots, a_m \mid q_1, \ldots, q_m)$. In this game, a referee decides whether the players win or lose according to a predetermined 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 $V(a_1, \ldots, a_m \mid q_1, \ldots, q_m) = 1$ and lose otherwise. 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 $1 \le i \le m$, 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

$$w(S) = \sum_{q_1,\ldots,q_m \in Q} \pi(q_1, \ldots, q_m) \sum_{a_1,\ldots,a_m \in A} S(a_1, \ldots, a_m \mid q_1, \ldots, q_m) V(a_1, \ldots, a_m \mid q_1, \ldots, q_m).$$

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 $w_{\mathrm{c}}(G)$ (resp. $w_{\mathrm{q}}(G)$, $w_{\mathrm{ns}}(G)$), is the supremum of the winning probabilities over all classical (resp. entangled, no-signaling) behaviors for G. Clearly we have $0 \le w_{\mathrm{c}}(G) \le w_{\mathrm{q}}(G) \le w_{\mathrm{ns}}(G) \le 1$. 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 $c, s\colon \mathbb{Z}_{\geq 0} \to [0,1]$. 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 $w_{\mathrm{c}}(G_x) \geq c(|x|)$ (resp. $w_{\mathrm{q}}(G_x) \geq c(|x|)$) 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 $w_{\mathrm{c}}(G_x) \leq s(|x|)$ (resp. $w_{\mathrm{q}}(G_x) \leq s(|x|)$) for all $x \notin L$.

Let $\mathrm{MIP}^*_{c(n),s(n)}(m,1)$ 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 $\mathrm{naPCP}_{c(n),s(n)}(r(n),q(n))$ 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 in a proof non-adaptively using $r(n)$ random bits.

Håstad [19] gave the following characterizations of NP and NEXP.

Theorem 3.2.1 (Håstad [19, Theorem 6.18])**.** *For any constant* $3/4 < s < 1$, $\mathrm{NP} = \bigcup_{c>0} \mathrm{naPCP}_{1,s}(c \log n, 3)$ *and* $\mathrm{NEXP} = \bigcup_{p \in \mathrm{poly}} \mathrm{naPCP}_{1,s}(p, 3)$.

3.3 Commuting-operator provers

3.3.1 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 study are actually valid even for this class. A *commuting-operator strategy* is a triplet $(\mathcal{H}, \rho, \mathcal{M}_q^{(i)})$ 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 $S(a_1, \ldots, a_m \mid q_1, \ldots, q_m) = \mathrm{tr}\, \rho M_{q_1,a_1}^{(1)} \cdots M_{q_m,a_m}^{(m)}$. 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 [40], and the entangled value of the game can be computed efficiently by using semidefinite programming. Tsirelson [40] also proved that this value does not change if we replace the entangled players by commuting-operator players. Tsirelson [41] 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 $\mathrm{tr}\,\rho \prod_{i\in P} X_{q_i}^{(i)}$ 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 3.3.1. *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. □

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).

3.3.2 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: $V(a_{\sigma(1)}, \ldots, a_{\sigma(m)} \mid q_{\sigma(1)}, \ldots, q_{\sigma(m)}) = V(a_1, \ldots, a_m \mid q_1, \ldots, q_m)$ 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 $M_{q,a}^{(i)} = I \otimes \cdots \otimes I \otimes M_{q,a}^{\prime(i)} \otimes I \otimes \cdots \otimes I$ 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 $M_q^{\prime(1)} = \cdots = M_q^{\prime(m)}$ for all $q \in Q$.

Lemma 3.3.2. *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.*

Proof. The lemma can be proved by constructing a symmetric strategy by averaging over all the permutations on provers. Detail follow.

Let $(\mathcal{H}, |\Psi\rangle, \mathcal{M}_q^{(i)})$ be a (not necessarily symmetric) commuting-operator strategy achieving acceptance probability p. Note that for any permutation $\tau \in \mathcal{S}_m$, the strategy $(\mathcal{H}, |\Psi\rangle, \mathcal{M}_q^{(\tau(i))})$ also achieves the same probability p because of the symmetry of the game.

We construct a symmetric strategy $(\mathcal{K}, |\Psi'\rangle, \mathcal{N}_q^{(i)})$ from the strategy $(\mathcal{H}, |\Psi\rangle, \mathcal{M}_q^{(i)})$. Let $\mathcal{K} = \mathcal{H} \otimes \mathbb{C}^{m!}$. We regard $\{|\tau\rangle \mid \tau \in \mathcal{S}_m\}$ as an orthonormal basis of $\mathbb{C}^{m!}$. We define a unitary representation Φ of the symmetric group $\mathcal{S}_m$ in $\mathcal{K}$ as $\Phi(\sigma)(|\varphi\rangle \otimes |\tau\rangle) = |\varphi\rangle \otimes |\tau\sigma^{-1}\rangle$. Now we define $|\Psi'\rangle \in \mathcal{K}$ by

$$|\Psi'\rangle = |\Psi\rangle \otimes \frac{1}{\sqrt{m!}} \sum_{\tau \in \mathcal{S}_m} |\tau\rangle.$$

The player i in the constructed symmetric strategy measures the $\mathbb{C}^{m!}$-part of the state, and acts just like the player $\tau(i)$ in the original strategy:

$$N_{q,a}^{(i)} = \sum_{\tau \in \mathcal{S}_m} M_{q,a}^{(\tau(i))} \otimes |\tau\rangle\langle\tau|.$$

This strategy is a commuting-operator strategy since, for $i \neq i'$,

$$\left[N_{q,a}^{(i)}, N_{q',a'}^{(i')}\right] = \sum_{\tau \in \mathcal{S}_m} \left[M_{q,a}^{(\tau(i))}, M_{q',a'}^{(\tau(i'))}\right] \otimes |\tau\rangle\langle\tau| = 0.$$

The symmetry of the strategy is verified as follows:

$$\Phi(\sigma)|\Psi'\rangle = |\Psi\rangle \otimes \frac{1}{\sqrt{m!}} \sum_{\tau \in \mathcal{S}_m} |\tau\sigma^{-1}\rangle = |\Psi'\rangle$$

and

$$\begin{aligned}
\Phi(\sigma^{-1}) N_{q,a}^{(\sigma(i))} \Phi(\sigma)(|\varphi\rangle \otimes |\tau\rangle) &= \Phi(\sigma^{-1}) N_{q,a}^{(\sigma(i))} \left(|\varphi\rangle \otimes |\tau\sigma^{-1}\rangle \right) \\
&= \Phi(\sigma^{-1}) \left(M_{q,a}^{(\tau(i))} |\varphi\rangle \otimes |\tau\sigma^{-1}\rangle \right) \\
&= M_{q,a}^{(\tau(i))} |\varphi\rangle \otimes |\tau\rangle \\
&= N_{q,a}^{(i)} (|\varphi\rangle \otimes |\tau\rangle).
\end{aligned}$$

In the constructed strategy, if measurement of the $\mathbb{C}^{m!}$-part of the shared state results in $\tau \in \mathcal{S}_m$, the players just follow the strategy $(\mathcal{H}, |\Psi\rangle, \mathcal{M}_q^{(\tau(i))})$, and therefore the strategy achieves winning probability p. □

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

3.4.1 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 [10], 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 [40].

The following theorem states that an upper bound for the value of the game $\mathrm{MS}_n(L)$ is also valid for MS_n.

Theorem 3.4.1. *For any Latin square L of order n, $w_{\mathrm{q}}(\mathrm{MS}_n) \leq w_{\mathrm{q}}(\mathrm{MS}_n(L))$ and $w_{\mathrm{com}}(\mathrm{MS}_n) \leq w_{\mathrm{com}}(\mathrm{MS}_n(L))$.*

Proof. First we prove that $w_{\mathrm{q}}(\mathrm{MS}_n) \leq w_{\mathrm{q}}(\mathrm{MS}_n(L))$. Consider an arbitrary entangled strategy S in the game MS_n. We construct an entangled strategy S' in the game $\mathrm{MS}_n(L)$ with the same winning probability as S.

Let $|\varphi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ be the state shared by the players in S. Without loss of generality, we assume that $\mathcal{H}_1 = \cdots = \mathcal{H}_n$. In S', the players share the state

$$|\varphi'\rangle = \frac{1}{\sqrt{n!}} \sum_{\sigma \in \mathcal{S}_n} U_\sigma |\varphi\rangle \otimes |\sigma(1)\rangle \otimes \cdots \otimes |\sigma(n)\rangle \in (\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n) \otimes (\mathbb{C}^n)^{\otimes n} \cong (\mathcal{H}_1 \otimes \mathbb{C}^n) \otimes \cdots \otimes (\mathcal{H}_n \otimes \mathbb{C}^n),$$

where $\mathcal{S}_n$ is the symmetric group on $\{1, \ldots, n\}$ and U_σ is the unitary operator on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ defined by $U_\sigma(|\varphi_1\rangle \otimes \cdots \otimes |\varphi_n\rangle) = |\varphi_{\sigma(1)}\rangle \otimes \cdots \otimes |\varphi_{\sigma(n)}\rangle$. Every player i holds the part of $|\varphi'\rangle$ corresponding to the space $\mathcal{H}_i \otimes \mathbb{C}^n$. When asked the content of the cell at row j, column k, the player $i = L_{jk}$ measures the $\mathbb{C}^n$-part of $|\varphi'\rangle$ in the computational basis to obtain the value of $\sigma(i)$, and acts like the player $\sigma(i)$ in S. This achieves the same winning probability as S.

The inequality $w_{\mathrm{com}}(\mathrm{MS}_n) \leq w_{\mathrm{com}}(\mathrm{MS}_n(L))$ can be proved similarly. Let S be a commuting-operator strategy in MS_n. Let $|\varphi\rangle \in \mathcal{H}$ be the state shared by the players in S, and $M_{jk}^{(i)} = (M_{jk,a}^{(i)})_{a \in \{0,1\}}$ be the POVM measured by player i when he is asked the content of the cell at row j, column k. Now we consider $\mathbb{C}^{n!}$ as a Hilbert space spanned by an orthonormal basis $\{|\sigma\rangle \mid \sigma \in \mathcal{S}_n\}$. In a strategy S' for $\mathrm{MS}_n(L)$, the commuting-operator players share the state

$$|\varphi\rangle \otimes \frac{1}{\sqrt{n!}} \sum_{\sigma \in \mathcal{S}_n} |\sigma\rangle \in \mathcal{H} \otimes \mathbb{C}^{n!}.$$

When asked the content of the cell at row j, column k, the player $i = L_{jk}$ measures $|\varphi'\rangle$ according to the POVM

$$N_{jk,a}^{(i)} = \sum_{\sigma \in \mathcal{S}_n} M_{jk,a}^{(\sigma(i))} \otimes |\sigma\rangle\langle\sigma|.$$

Note that if $L_{jk} = i \neq i' = L_{j'k'}$, then $N_{jk,a}^{(i)}$ and $N_{j'k',a'}^{(i')}$ commute as required in the commuting-operator model since

$$\left[N_{jk,a}^{(i)}, N_{j'k',a'}^{(i')}\right] = \sum_{\sigma \in \mathcal{S}_n} \left[M_{jk,a}^{(\sigma(i))}, M_{j'k',a'}^{(\sigma(i'))}\right] \otimes |\sigma\rangle\langle\sigma| = 0. \qquad \square$$

3.4.2 A strategy for entangled players

Theorem 3.4.2. *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

$$\begin{aligned} Z_\theta &= \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}. \end{aligned}$$

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

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

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 prepare the following lemma.

Lemma 3.4.3. *Let $n \ge 1$ and $\theta_1, \dots, \theta_n \in \mathbb{R}$, and let $|\varphi_n\rangle$ and Z_θ as defined above. Let $M = Z_{\theta_1} \otimes \cdots \otimes Z_{\theta_n}$. Then,*

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

Proof. Let

$$|\varphi'_n\rangle = \frac{1}{2^{(n-1)/2}}\Big(\sum_{\substack{x\in\{0,1\}^n \\ W(x)\equiv 1 \bmod 4}} |x\rangle - \sum_{\substack{x\in\{0,1\}^n \\ W(x)\equiv 3 \bmod 4}} |x\rangle\Big).$$

We actually prove the following stronger statement:

$$\begin{aligned} \langle\varphi_n|M|\varphi_n\rangle = -\langle\varphi'_n|M|\varphi'_n\rangle &= \cos(\theta_1 + \cdots + \theta_n), \\ \langle\varphi_n|M|\varphi'_n\rangle = \langle\varphi'_n|M|\varphi_n\rangle &= \sin(\theta_1 + \cdots + \theta_n). \end{aligned}$$

The proof is by induction on n. The case $n = 1$ holds by the definition of Z_{θ_1}. If $n > 1$, note that

$$\begin{aligned} |\varphi_n\rangle &= \frac{1}{\sqrt{2}}(|\varphi_{n-1}\rangle \otimes |0\rangle - |\varphi'_{n-1}\rangle \otimes |1\rangle), \\ |\varphi'_n\rangle &= \frac{1}{\sqrt{2}}(|\varphi'_{n-1}\rangle \otimes |0\rangle + |\varphi_{n-1}\rangle \otimes |1\rangle). \end{aligned}$$

Let $N = Z_{\theta_1} \otimes \cdots \otimes Z_{\theta_{n-1}}$. Then,

$$\begin{aligned}\langle\varphi_n|M|\varphi_n\rangle &= \frac{1}{2}(\langle\varphi_{n-1}|N|\varphi_{n-1}\rangle\langle 0|Z_{\theta_n}|0\rangle + \langle\varphi'_{n-1}|N|\varphi'_{n-1}\rangle\langle 1|Z_{\theta_n}|1\rangle \\ &\qquad - \langle\varphi_{n-1}|N|\varphi'_{n-1}\rangle\langle 0|Z_{\theta_n}|1\rangle - \langle\varphi'_{n-1}|N|\varphi_{n-1}\rangle\langle 1|Z_{\theta_n}|0\rangle) \\ &= \cos(\theta_1 + \cdots + \theta_{n-1})\cos\theta_n - \sin(\theta_1 + \cdots + \theta_{n-1})\sin\theta_n \\ &= \cos(\theta_1 + \cdots + \theta_{n-1} + \theta_n).\end{aligned}$$

The other three equalities are proved similarly. □

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 3.4.3, 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.

3.4.3 Optimality of the strategy

We prove the following theorem in this section, and relate it to the n-player Magic Square game.

Theorem 3.4.4. *Let $X_j^{(i)}$ be ±1-valued observables on $\mathcal{H}$ for $0 \le i \le n-1$ and $1 \le j \le n$ where $X_j^{(i)}$ and $X_{j'}^{(i')}$ commute if $i \neq i'$ ($\forall 1 \le j, j' \le n$). 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 $1 \le j, k \le n$, where the subscript $k - i$ is interpreted under modulo n. Then,*

$$\sum_{j=1}^{n}\langle M_j\rangle + \sum_{k=1}^{n-1}\langle N_k\rangle - \langle N_n\rangle \le 2n\cos\frac{\pi}{2n}, \tag{3.1}$$

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

For $n = 3$, Theorem 3.4.4 gives the following Tsirelson-type inequality.

Corollary 3.4.5. *Let $X_j^{(i)}$ be ±1-valued observables on $\mathcal{H}$ for $1 \le i, j \le 3$ where $X_j^{(i)}$ and $X_{j'}^{(i')}$ commute if $i \neq i'$ ($\forall 1 \le j, j' \le 3$). Then,*

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

We use the following lemma to prove Theorem 3.4.4.

Lemma 3.4.6. *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 $\left|\langle\varphi|AB|\varphi\rangle - \alpha\beta\right| \le \sqrt{1-|\alpha|^2}\sqrt{1-|\beta|^2}$.*

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

$$|\psi\rangle = \frac{B|\varphi\rangle - \beta|\varphi\rangle}{\sqrt{1-|\beta|^2}}.$$

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 $\left|\langle\varphi|AB|\varphi\rangle - \alpha\beta\right|^2 = \left|\langle\varphi|A|\psi\rangle\right|^2(1-|\beta|^2) \leq (1-|\alpha|^2)(1-|\beta|^2)$. □

Corollary 3.4.7. *Let $\mathcal{H}$, $|\varphi\rangle$, A, B, α and β be as defined in Lemma 3.4.6. 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 3.4.6,

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

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 $\sin\theta, \sin\theta' \geq 0$. □

Corollary 3.4.8. *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 3.4.7 repeatedly. □

Proof of Theorem 3.4.4. 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 $P = \prod_{j=1}^n M_j N_{n+1-j} = M_1 N_n M_2 N_{n-1}\cdots M_n N_1$.[1] We prove that $P = I$. For $i = 0, \ldots, n-1$, let

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

[1] Here $\prod_{j=1}^n O_j$ denotes the product $O_1 O_2 \cdots O_n$ of operators. This is a slight abuse of the notation since the operators do not necessarily commute.

Note that $P = P_0P_1 \cdots P_{n-1}$, 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 $P_i = Y_1Y_2 \cdots Y_{2n}$. 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 $Y_1Y_2 \cdots Y_{2(n-i)} = Y_1(Y_2 \cdots (Y_{n-i}Y_{n-i+1}) \cdots Y_{2(n-i)-1})Y_{2(n-i)} = I$. 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 $M_1(-N_n)M_2N_{n-1}M_3N_{n-2} \cdots M_nN_1 = -P = -I$, it holds that $\sum_{j=1}^n \theta_j + \sum_{k=1}^n \theta'_k \geq \pi$ by Corollary 3.4.8. As is shown in the following Lemma 3.4.9, $\langle\varphi|Z|\varphi\rangle \leq 2n\cos(\pi/(2n))$ subject to this constraint, which establishes Theorem 3.4.4. □

Lemma 3.4.9. *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 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 $\pi/2 \leq \theta_1 \leq \pi$,

$$\begin{aligned}\cos\theta_1 + \cdots + \cos\theta_n &\leq \cos\theta_1 + (n-1)\cos\frac{\pi-\theta_1}{n-1} \\ &< \cos\frac{\pi}{2} + (n-1)\cos\frac{\pi}{2(n-1)} < n\cos\frac{\pi}{n}.\end{aligned}$$

□

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.

Corollary 3.4.10. *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 $(1 + \cos\frac{\pi}{2n})/2$.*

Proof. Note that the inequality (3.1) 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 3.4.10 follows from Theorems 3.4.4, 3.4.1 and 3.4.2. □

We note that Theorem 3.4.4 includes the following inequality proved by Wehner [44] as special cases.

Theorem 3.4.11 (Wehner [44]). *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,*

$$\sum_{j=1}^{n} \langle X_j Y_j \rangle + \sum_{j=1}^{n-1} \langle X_{j+1} Y_j \rangle - \langle X_1 Y_n \rangle \leq 2n \cos \frac{\pi}{2n}. \tag{3.2}$$

Proof. In the inequality (3.1), 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 (3.1) is exactly the same as the inequality (3.2). □

The equality in (3.2) is achievable [33]. 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 3.4.1. 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 3.4.10 since $w_{\mathrm{ns}}(\mathrm{MS}_n) = 1$. This follows from the result by Barrett and Pironio [5, 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 3.4.2. 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 3.4.10 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}.

3.5 Three-prover proof system based on three-query PCP

Let $\mathrm{naPCP}_{c(n),s(n)}(r(n), q(n))$ 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 $\mathrm{MIP}^*_{c(n),s(n)}(m, 1)$ 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 3.5.1. *There exists a constant $c_1, c_2 > 0$ such that for any functions $\varepsilon\colon \mathbb{Z}_{\geq 0} \to (0,1)$ and $r\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ and any language $L \in \mathrm{naPCP}_{1,1-\varepsilon(n)}(r(n),3)$, L has a three-prover one-round interactive proof system which satisfies the following conditions.*

(a) The proof system is binary*, i.e. the verifier receives only one bit from each prover.*

(b) The verifier uses $r(n) + O(1)$ random bits.

(c) The verifier receives only one bit from each prover.

(d) The completeness holds perfectly with classical provers.

(e) If dishonest provers are classical, the soundness acceptance probability is at most $1 - c_1\varepsilon(n)$.

(f) If dishonest provers are commuting-operator, the soundness acceptance probability is at most $1 - \varepsilon_{\mathrm{q}}(n)$, where $\varepsilon_{\mathrm{q}}(n) = c_2\varepsilon(n)^2 \cdot 2^{-2r(n)}$.

This implies $\mathrm{naPCP}_{1,1-\varepsilon(n)}(r(n),3) \subseteq \mathrm{MIP}^*_{1,1-\varepsilon_{\mathrm{q}}(n)}(3,1)$.

Letting $c_1 = 1/8$ and $c_2 = 1/384$ suffices for our proof. We do not attempt to maximize c_1 or c_2.

By applying Theorem 3.5.1 to the PCP systems of Theorem 3.2.1, we obtain the following corollaries.

Corollary 3.5.2. *There exists a constant $0 < \varepsilon < 1$ and a polynomially bounded function $p\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 1}$ such that the following promise problem is NP-complete.*

> ***Instance*** *A classical three-player one-round binary-answer game G with n questions, given as a description of a probability distribution over triplets of questions and a table showing whether the answers are accepted or not for each triplet of questions and each triplet of answers.*
>
> ***Yes-promise*** $w_{\mathrm{c}}(G) = 1$.
>
> ***No-promise*** $w_{\mathrm{c}}(G) \leq \varepsilon$ *and* $w_{\mathrm{com}}(G) \leq 1 - 1/p(n)$.

Corollary 3.5.3. $\mathrm{NEXP} \subseteq \bigcup_{p\in\mathrm{poly}} \mathrm{MIP}^*_{1,1-2^{-p}}(3,1)$*, where each prover answers one bit, honest provers do not need to share prior entanglement, and the soundness error becomes some constant if provers are restricted to classical.*

3.5.1 Construction of proof system and basic facts

Let $L \in \mathrm{naPCP}_{1,1-\varepsilon(n)}(r(n), 3)$. 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.

The properties (a), (b) and (c) of Theorem 3.5.1 are obvious from the construction. This interactive proof system clearly achieves perfect completeness with honest provers answering the asked bit in the proof, thus part (d) holds.

We proceed to part (e). Let x be an input string with $|x| = n$, and suppose that there exists a strategy for the three unentangled provers to achieve the acceptance probability at least $1 - \varepsilon(n)/8$. This strategy is accepted in each of the consistency test and the simulation test with probability at least $1 - \varepsilon(n)/4$. We may assume without loss of generality that the strategy is deterministic. For $1 \leq i \leq 3$ and $q \in Q$, let $f_i(q)$ be the answer given by the prover i when he/she is asked the question q.

Let $y = y_1 \cdots y_N$ be a string consisting of the answers of the prover 1: $y_q = f_1(q)$ for all $q \in Q$. We prove that using y as PCP certificate makes the PCP verifier accept with probability at least $1 - \varepsilon(n)$. A question $q \in Q$ is said to be *good* if $f_1(q) = f_2(q) = f_3(q)$, and *bad* otherwise. Suppose the PCP verifier has chosen three questions $q_1, q_2, q_3 \in Q$. If all the three questions are good *and* the PCP verifier rejects, then the verifier in the constructed three-prover system must reject in the simulation test in the same situation. However, this happens with probability at most $\varepsilon(n)/4$. On the other hand, each of the three questions is good with probability at least $1-\varepsilon(n)/4$, and therefore at least one question is bad with probability at most $3\varepsilon(n)/4$. Therefore, the PCP verifier can reject at most $\varepsilon(n)/4 + 3\varepsilon(n)/4 = \varepsilon(n)$.

By soundness property of the PCP system, this implies $x \in L$, and therefore our three-prover system has soundness acceptance probability at most $1 - \varepsilon(n)/8$. This proves part (e).

In the rest of this section, we will prove part (f), i.e. we will show that the soundness acceptance probability of this interactive proof system with any commuting-operator provers is at most $1 - (1/384)(1 - s(n))^2 \cdot 2^{-2r(n)}$.

Our soundness analysis to prove Theorem 3.5.1 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 [25].

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 $f = (x_1 \oplus x_3 \oplus x_5) \wedge (\overline{x_1 \oplus x_4 \oplus x_6}) \wedge (\overline{x_2 \oplus x_3 \oplus x_6}) \wedge (\overline{x_2 \oplus x_4 \oplus x_5})$, where $\oplus$ denotes the exclusive OR.

3.5.2 Impossibility of perfect cheating

Before proceeding to the proof of Theorem 3.5.1, 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 [35] with a different proof. We provide 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 3.3.1. 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,

$$M_{q,a}^{(1)}|\Psi\rangle = M_{q,a}^{(2)}|\Psi\rangle = M_{q,a}^{(3)}|\Psi\rangle \tag{3.3}$$

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 3.5.1. *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. □

Claim 3.5.2. *The $6n$ projectors $M_{q,a}^{(i)}$ pairwise commute on $\mathcal{H}'$.*

Proof. Let $|\varphi\rangle \in \mathcal{H}'$. By Claim 3.5.1, $M_{q,a}^{(1)}M_{q',a'}^{(1)}|\varphi\rangle = M_{q,a}^{(1)}M_{q',a'}^{(3)}|\varphi\rangle = M_{q',a'}^{(3)}M_{q,a}^{(1)}|\varphi\rangle = M_{q',a'}^{(3)}M_{q,a}^{(2)}|\varphi\rangle = M_{q,a}^{(2)}M_{q',a'}^{(3)}|\varphi\rangle = M_{q,a}^{(2)}M_{q',a'}^{(1)}|\varphi\rangle = M_{q',a'}^{(1)}M_{q,a}^{(2)}|\varphi\rangle = M_{q',a'}^{(1)}M_{q,a}^{(1)}|\varphi\rangle$. 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. □

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 3.5.2, these $6n$ operators are pairwise commuting Hermitian operators when restricted to $\mathcal{H}'$. By Lemma 3.3.1, 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 3.5.1. A statement analogous to Claim 3.5.2 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 $M^{(1)}_{q,1} = M_q \otimes I$, $M^{(2)}_{q,1} = I \otimes (I - M_q)$ for $q = 1, 2$. Then $M^{(1)}_{q,a}|\Psi\rangle = M^{(2)}_{q,a}|\Psi\rangle$ for $q \in \{1, 2\}$ and $a \in \{0, 1\}$ whereas $M^{(1)}_{1,a} M^{(1)}_{2,a'}|\Psi\rangle \neq M^{(1)}_{2,a'} M^{(1)}_{1,a}|\Psi\rangle$.

3.5.3 Proof of part (f) of Theorem 3.5.1

In the case of imperfect cheating, the equalities in (3.3) 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 (3.3) implies that measurements $\mathcal{M}^{(i)}_q$ are almost commuting on the shared state $|\Psi\rangle$.

Kempe, Kobayashi, Matsumoto, Toner and Vidick [25] 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 disturb the reduced state shared by them so much (Claim 20 in [24]), 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 $|\Psi\rangle$.

Lemma 3.5.4. *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*

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

$$\Delta = \sum_{i=1}^{v} \left\| \sqrt{M_i}\rho\sqrt{M_i} - \sqrt{N_i}\rho\sqrt{N_i} \right\|_1.$$

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

Proof. Let $X_i = \sqrt{M_i}$ and $Y_i = \sqrt{N_i}$. We define linear operators $U, V \colon \mathcal{H} \to \mathcal{H} \otimes \mathbb{C}^v$ by

$$U \colon |\varphi\rangle \mapsto \sum_{i=1}^{v} X_i|\varphi\rangle \otimes |i\rangle,$$
$$V \colon |\varphi\rangle \mapsto \sum_{i=1}^{v} Y_i|\varphi\rangle \otimes |i\rangle.$$

It is easy to check $U^*U = V^*V = I$. Using these operators, Δ can be written as $\Delta = 2D(U\rho U^*, V\rho V^*)$.

First we prove the case where ρ is a pure state: $\rho = |\Psi\rangle\langle\Psi|$. In this case,

$$\begin{aligned}\Delta^2 = 4D(U|\Psi\rangle\langle\Psi|U^*, V|\Psi\rangle\langle\Psi|V^*)^2 &= 4(1 - |\langle\Psi|U^*V|\Psi\rangle|^2) \\ &= 4(1 + |\langle\Psi|U^*V|\Psi\rangle|)(1 - |\langle\Psi|U^*V|\Psi\rangle|) \\ &\le 8(1 - \Re(\langle\Psi|U^*V|\Psi\rangle)) \\ &= 8\lambda.\end{aligned}$$

If ρ is a mixed state, decompose ρ to a convex combination of pure states: $\rho = \sum_{j=1}^{n} p_j\rho_j$. Let

$$\lambda_j = \frac{1}{2}\sum_{i=1}^{v} \operatorname{tr}\rho_j(X_i - Y_i)^2,$$
$$\Delta_j = \sum_{i=1}^{v} \|X_i\rho_j X_i - Y_i\rho_j Y_i\|.$$

Then,

$$\Delta \le \sum_{j=1}^{n} p_j\Delta_j \le \sum_{j=1}^{n} p_j \cdot 2\sqrt{2\lambda_j} \le 2\sqrt{2\lambda}. \qquad \square$$

We fix an input $x \notin L$. Let $Q \subseteq \mathbb{Z}_{\ge 1}$ 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 $|Q| \le 3 \cdot 2^r$. 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 3.3.2, we can assume that this strategy is symmetric without loss of generality. Let $|\Psi\rangle$ be the quantum state shared by the provers. For $1 \le i \le 3$ 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 $M^{(i)}_{q,0} = I$ and $M^{(i)}_{q,1} = 0$ 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

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

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

$$\begin{aligned}
\lambda_q &= 1 - \sum_{a\in\{0,1\}} \langle\Psi|M^{(1)}_{q,a}M^{(2)}_{q,a}|\Psi\rangle \\
&= 1 - \sum_{a\in\{0,1\}} \langle\Psi|M^{(2)}_{q,a}M^{(3)}_{q,a}|\Psi\rangle \\
&= 1 - \sum_{a\in\{0,1\}} \langle\Psi|M^{(3)}_{q,a}M^{(1)}_{q,a}|\Psi\rangle .
\end{aligned}$$

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

$$\begin{aligned}
w_{\mathrm{cons}} &= \sum_{q\in Q} \pi_q \Big(P_{\mathrm{com}}(0,0,0 \mid q,q,q) + P_{\mathrm{com}}(1,1,1 \mid q,q,q) \Big) \\
&= \sum_{q\in Q} \pi_q \left(\langle\Psi|M^{(1)}_{q,0}M^{(2)}_{q,0}M^{(3)}_{q,0}|\Psi\rangle + \langle\Psi|M^{(1)}_{q,1}M^{(2)}_{q,1}M^{(3)}_{q,1}|\Psi\rangle \right) \\
&= \sum_{q\in Q} \pi_q \frac{\sum_{a\in\{0,1\}} (\langle\Psi|M^{(1)}_{q,a}M^{(2)}_{q,a}|\Psi\rangle + \langle\Psi|M^{(2)}_{q,a}M^{(3)}_{q,a}|\Psi\rangle + \langle\Psi|M^{(3)}_{q,a}M^{(1)}_{q,a}|\Psi\rangle) - 1}{2} = 1 - \frac{3}{2}\sum_{q\in Q} \pi_q \lambda_q , \\
w_{\mathrm{sim}} &= \sum_{q_1,q_2,q_3\in Q} \pi(q_1,q_2,q_3) \sum_{a_1,a_2,a_3\in\{0,1\}} P_{\mathrm{com}}(a_1,a_2,a_3 \mid q_1,q_2,q_3) V(a_1,a_2,a_3 \mid q_1,q_2,q_3).
\end{aligned}$$

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

$$w_{\mathrm{cons}} \leq 1 - \frac{1}{2 \cdot 2^r} \sum_{q\in Q} \lambda_q . \tag{3.4}$$

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

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

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

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

By the soundness condition of the PCP system,

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

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

$$P'(a_1,a_2,a_3 \mid q_1,q_2,q_3) = \|M^{(i)}_{q'_1,a'_1} M^{(i)}_{q'_2,a'_2} M^{(i)}_{q'_3,a'_3} |\Psi\rangle\|^2,$$

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

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

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 $p_0, \ldots, p_l$ 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.[2] For $0 \le q \le l$ and $y \in \{0,1\}^l$, let

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

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

$$\sum_{\substack{y\in\{0,1\}^l \\ y_{q_1}=a_1, y_{q_2}=a_2, y_{q_3}=a_3}} p_0(y) = P_{\mathrm{c}}(a_1,a_2,a_3 \mid q_1,q_2,q_3),$$

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

Let $1 \le q \le l$. By Lemma 3.5.4, we have

$$\sum_{y_q\in\{0,1\}} \left\| M^{(3)}_{q,y_q} |\Psi\rangle\langle\Psi| M^{(3)}_{q,y_q} - M^{(i_q)}_{q,y_q} |\Psi\rangle\langle\Psi| M^{(i_q)}_{q,y_q} \right\|_1 \le 2\sqrt{2\lambda_q}.$$

[2] 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,

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

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,

$$\sum_{a_1,a_2,a_3\in\{0,1\}} \sum_{\substack{y\in\{0,1\}^l \\ y_{q_1}=a_1, y_{q_2}=a_2, y_{q_3}=a_3}} |p_0(y) - p_l(y)| \le \sum_{q=1}^{l} 2\sqrt{2\lambda_q}.$$

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

Claim 3.5.2. *For distinct $q_1, q_2, q_3 \in Q$,*[3]

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

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

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

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

each of which follows from Lemma 3.5.4, and use the triangle inequality. The other cases are proved similarly, where we use $P'(a_1,a_2,a_3 \mid q_1,q_2,q_3) = \|M^{(i)}_{q_1,a_1} M^{(i)}_{q_2,a_2} M^{(i)}_{q_3,a_3}|\Psi\rangle\|^2$ with i such that q_i is the smallest in q_1, q_2, q_3. □

[3] Actually, we can omit the term $2\sqrt{2\lambda_{q_i}}$ from the right-hand side of the inequality, where $q_i = \min\{q_1, q_2, q_3\}$.

By Claims 3.5.1 and 3.5.2, for any distinct $q_1, q_2, q_3 \in Q$,

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

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

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

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

3.5.4 The two-prover case

Finally, the result by Cleve, Høyer, Toner and Watrous [13] 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.

Theorem 3.5.5. *(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* $1 - 2^{-\mathrm{poly}}$.

Proof. (i) For a two-player one-round binary-answer game G, $w_{\mathrm{q}}(G) = 1$ if and only if $w_{\mathrm{c}}(G) = 1$ [13, 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. □

[4]The first inequality is shown as follows. Let $c = 8\sqrt{3}\cdot 2^r$, $t = 1 - w_{\mathrm{sim}}$, $u = \sqrt{1-w_{\mathrm{cons}}}$. Then $8\sqrt{6}\cdot 2^r\sqrt{1-w} = c\sqrt{t+u^2}$. Since $c \geq 8\sqrt{3}$, it follows that $c^2(t+u^2) - (t+cu)^2 = c^2t - t^2 - 2ctu \geq t(c^2 - t - 2c) \geq t(c^2 - 1 - 2c) \geq 0$, or $c\sqrt{t+u^2} \geq t + cu = 1 - w_{\mathrm{sim}} + 8\sqrt{3}\cdot 2^r\sqrt{1-w_{\mathrm{cons}}}$.

Chapter 4

General Non-Local Correlations

4.1 Motivation

Entanglement, superposition and negative amplitudes are three fundamental properties of quantum mechanics and quantum computation. The relation of superposition and negative amplitudes to computation can be studied in the context of quantum algorithms - this is the "intuition" behind the fact that some quantum algorithms outperform the classical ones. Entanglement, on the other hand, is best studied not only in a strictly quantum mechanical framework (e.g. state teleportation, no-cloning theorem, etc), but also in communication.

The communication model we will study is that of multiprover interactive proofs and games. These proof systems have many connections with other areas in theoretical computer science, like inapproximability / hardness of approximation results, probabilistic checkable proofs, cryptography, etc.

The class MIP (multiprover interactive proofs) is defined as the set of all languages that can be decided by a polynomial time verifier by interacting with several computationally unbounded provers that do not communicate with each other. Informally, the goal of the provers is to convince the verifier that a string has a certain property. They should succeed when the string indeed has the property, and fail otherwise.

Because the intuition behind MIP is to bound the power of the verifier and not that of the provers, the latter may be allowed to share quantum entanglement. The verifier and its communication with the provers remain classical, but now the provers can use the entanglement to obtain stronger-than-classical correlations. There are several reasons to study entanglement and interactive proof together. First, it may give new insights regarding the power of entanglement. Second, quantum arguments have begun to play a significant role in proving classical complexity results. From this point of view, we also hope to get a better understanding of MIP and its connections to other areas.

4.2 Introduction

It has been shown by Babai et al [2] that any language in NEXP has a two-prover interactive proof system. This result has been improved by Feige and Lovasz [16] by showing that a language is in NEXP if and only if it has a two-prover, one round interactive proof with perfect completeness and exponentially small soundness error. Recently, Cleve et all [11] showed that NEXP is equal to MIP with two provers, one round, one-bit answers, the verifier only looks at the XOR of these bits, and some specific values of the correctness and soundness error (call this class $\oplus MIP[2](c, s)$)

The only known result when one allows quantum correlations between the provers is that of Wehner [43] that $\oplus MIP[2](c, s)$ with quantum correlations is included in $QIP(2) \in EXP$ for any choice of c and s.

Another interesting question is to allow the provers to have access to arbitrary non-local correlations. The only constraint is non-communication among the provers, i.e. for any prover, the distribution of its answer to a given question is independent on the questions sent to the other provers. This model has been introduced by Popescu and Rohrlich [34] and further studied by Barrett et all [4]. Although there is no physical implementation of this model so far, the question that arises is: Is there any reason why these correlations haven't been observed in nature? One way to answer this question is to see what would happen from a computational or information-theoretical point of view if these "perfect" correlations existed. Buhrman and Massar [8] showed that if these correlations can be realized using quantum operations, then they lead to super-luminal communication. They conjecture that reversibility might be one of the reasons that stronger-than-quantum correlations do not exist.

4.3 Total Non-Local Correlations

We will show that if we allow the provers to share arbitrary non-local correlations, $\oplus MIP = PSPACE$ (MIP with the verifier looking at the bitwise XOR of the provers' answers), and in particular $\oplus MIP[2](c, s)$ is contained in AM. The idea is similar to the one used by van Dam [42] to show that the communication complexity of any two-party boolean function is 1 bit if total non-local correlations are allowed.

Definition 4.3.1. Consider n parties with inputs x_i and outputs y_i. We say that these parties have access to total non-local correlations if for any i, $Pr[y_i = a]$ depends only on x_i for all allowed values of a.

Basic non-local box: There is a non-local box that on inputs x and y outputs a and b such that $a \oplus b = xy$

Consider two parties Alice and Bob, who receive x_1 and x_2 respectively. The goal is to output y_1 and y_2 such that $y_1 \oplus y_2 = x_1 x_2$, using no communication. Classically (i.e. with share randomness), $Pr[y_1 \oplus y_2 = x_1 x_2] \leq 3/4$. However, theoretically this relationship can hold with probability 1: if input $x_1 x_2 \in \{00, 01, 10\}$, the output is 00 or 11 with equal probability. If the input is 11, the output is 01 or 10 with equal probability. It is easy to see that this distribution satisfies the

no-communication requirement (the probability of each individual output depends only on the corresponding input - the probability that each output bit is 0 is constant 1/2)

Claim 4.3.1. *Any Boolean function f of n variables can be written as the XOR of (product) monomials, each appearing with coefficient 1 or 0*

Proof. By induction. It is true for any function on 1 variable. Suppose it is true for all functions on $n-1$ variables. Any Boolean function on n variables can be written as: $f(x_1, x_2, ..., x_n) = x_n g(x_1, ..., x_{n-1}) \oplus (1 \oplus x_n) h(x_1, ..., x_{n-1}) = h \oplus x_n(f \oplus h)$

h is an XOR of monomials all with coefficients 0 or 1 (by induction hypothesis), $f \oplus h$ is another Boolean function on $n-1$ variables and hence also an XOR of monomials all with coefficients 0 or 1. □

Claim 4.3.2. *Using the basic non-local box that on input x, y outputs a, b such that $a \oplus b = xy$, we can construct a (non-local) box that on input $x_1, ..., x_n$ outputs $a_1, ..., a_n$ such that $a_1 \oplus ... \oplus a_n = x_1 ... x_n$*

Proof. By induction: suppose it's true for $n-1$ variables, add another one. So we have $a_1 \oplus ... \oplus a_{n-1} = x_1 ... x_{n-1}$ This means that $x_1 ... x_n = a_1 x_n \oplus ... \oplus a_{n-1} x_n = a'_1 \oplus a_{n,1} \oplus ... \oplus a'_{n-1} \oplus a_{n,n-1} = a'_1 \oplus ... \oplus a_{n-1} \oplus a_n$ In the last step we used the non-local box on inputs a_1 and x_n, etc up to a_{n-1} and x_n and then group variables together. □

Claim 4.3.3. *A set of n machines (provers) that don't communicate but have access to full non-local correlations, on input $q_1, ..., q_n$ can output bits $b_1, ..., b_n$ such that $b_1 \oplus ... \oplus b_n$ can define any Boolean function on $q_1, ...q_n$*

Proof. Using Claims 2&3 above, each prover can obtain sets $a_1 ... a_k$ for each monomial, then each prover XORs its a's and outputs the answer. □

Definition 4.3.2.

- Let **MIP** be the class of languages such that ∃ polynomial time verifier V such that: $x \in L$ then ∃ prover P such that $Pr[V(x, P) accepts] \geq c$; $x \notin L$ then ∀ provers P $Pr[V(x, P) accepts] \leq s$
- Let $\oplus$**MIP** be a class similar to **MIP**, except that the verifier $V_\oplus$ doesn't look at individual prover answers in a given round, but only at the bit-wise XOR (assume all answers have the same length)
- Let $\mathbf{MIP_{NL}}$ be equal to **MIP** when provers share total non-local correlations

Theorem 4.3.3. *For any verifier $V_\oplus$ and any k-round protocol involving n communicating provers P^{COMM}, there is a set of non-local provers P^{NL} such that the acceptance probability is the same.*

Proof. We'll prove that there is a set P^{NL} that for each given questions $q_1 ... q_n$ to the provers, give the same behavior of the verifier.

Consider the $(V_\oplus, P^{COMM})$ protocol. At each round, the provers return the answers $r_1 ... r_n$. Let $b_1 ... b_l$ be the bit-wise XOR of these answers (the only thing that counts from the point of view of

the verifier) (l = length of provers' answers). Each b_i is a Boolean function of the questions asked so far to all provers, and hence can be simulated by a set of non-local provers. So, there is a set of non-local provers that can create the same $b_1...b_l$ and that would make the verifier accept with the same probability. □

Theorem 4.3.4. $\oplus\mathbf{MIP_{COMM}} = \oplus\mathbf{MIP_{NL}}$

Proof. $L \in \oplus\mathbf{MIP_{COMM}}$ iff $\exists V_\oplus$ such that:

- $x \in L$ => $\exists P_i^{COMM}$ such that Pr[$(V_\oplus, P_i^{COMM})$ acc.] $\geq c$
- $x \notin L$ => $\forall P_i^{COMM}$ Pr[$(V_\oplus, P_i^{COMM})$ acc.] $\leq s$

$L \in \oplus\mathbf{MIP_{NL}}$ iff $\exists V'_\oplus$ such that:

- $x \in L$ => $\exists P_i^{NL}$ such that Pr[$(V'_\oplus, P_i^{NL})$ acc.] $\geq c$
- $x \notin L$ => $\forall P_i^{NL}$ Pr[$(V'_\oplus, P_i^{NL})$ acc.] $\leq s$

" =>": Let $V'_\oplus = V_\oplus$

Let $x \in L \in \oplus\mathbf{MIP_{COMM}}$ Then $\exists P_i^{COMM}$ such that Pr[$(V_\oplus, P_i^{COMM})$ acc.] $\geq c$. Using Theorem 5, we obtain that $\exists P_i^{NL}$ such that Pr[$(V_\oplus, P_i^{NL})$ acc.] $\geq c$

Let $x \notin L \in \oplus\mathbf{MIP_{COMM}}$ Then $\forall P_i^{COMM}$ Pr[$(V_\oplus, P_i^{COMM})$ acc.] $\leq s$ => $\forall P_i^{NL}$ Pr[$(V_\oplus, P_i^{NL})$ acc.] $\leq s$

" <=": Let $V'_\oplus = V_\oplus$

Let $x \in L \in \oplus\mathbf{MIP_{NL}}$ Then $\exists P_i^{NL}$ such that Pr[$(V_\oplus, P_i^{NL})$ acc.] $\geq c$ => $\exists P_i^{COMM}$ such that Pr[$(V_\oplus, P_i^{COMM})$ acc.] $\geq c$

Let $x \notin L \in \oplus\mathbf{MIP_{NL}}$ Then $\forall P_i^{NL}$ Pr[$(V_\oplus, P_i^{NL})$ acc.] $\leq s$ Suppose $\exists P_i^{COMM}$ such that Pr[$(V_\oplus, P_i^{COMM})$ acc.] $> s$ Using Theorem 5, we obtain that $\exists P_i^{NL}$ such that Pr[$(V_\oplus, P_i^{NL})$ acc.] $> s$, contradiction. So, $\forall P_i^{COMM}$ Pr[$(V_\oplus, P_i^{COMM})$ acc.] $\leq s$ □

Theorem 4.3.5. $\mathbf{IP} = \oplus\mathbf{MIP_{COMM}}$

Proof. $L \in \mathbf{IP}$ iff $\exists V$ such that:

- if $x \in L$ then $\exists P$ such that Pr[(V, P) acc] $\geq c$
- if $x \notin L$, then $\forall P$, Pr[(V, P) acc] $\leq s$

" =>" Let V' the $\oplus\mathbf{MIP_{COMM}}$ verifier be such that it behaves exactly like the **IP** verifier, except it sends the question to prover 1 and a fixed question to all the others.

Let $x \in L \in \mathbf{IP}$ Then $\exists P$ such that Pr[(V, P) acc] $\geq c$. Let $P_1^{COMM} = P$ and all other P_i^{COMM} just return O^l Then Pr[(V', P_i^{COMM}) acc] $\geq c$.

Let $x \notin L \in \mathbf{IP}$ Then, $\forall P$, Pr[(V, P) acc] $\leq s$ Suppose there is a set P_i^{COMM} such that Pr[(V', P_i^{COMM}) acc] $\geq s$ We could build a P that behaves the same way, contradiction.

" <=" Let V' the **IP** verifier be such that it is identical to the $\oplus\mathbf{MIP_{COMM}}$ verifier after it computes the XOR of the provers' answers (and asks all questions to the only prover)

Let $x \in L \in \oplus\mathbf{MIP_{COMM}}$ Then $\exists P_i^{COMM}$ such that Pr[(V, P_i^{COMM}) acc.] $\geq c$. Let P simulate the behavior of P_i^{COMM}'s and then take the XOR. We have: Pr[(V', P) acc] $\geq c$

Let $x \notin L \in \oplus\mathbf{MIP_{COMM}}$ Then $\forall P_i^{COMM}$ Pr[(V, P_i^{COMM}) acc.] $\leq s$ Suppose $\exists P$ such that Pr[(V', P) acc] $\geq s$. But P could be simulated by P_i^{COMM}, contradiction. □

Corollary 4.3.6. $\oplus\mathbf{MIP_{NL}} = \mathbf{IP}$ *and* $\oplus\mathbf{2IP_{NL}} = \mathbf{AM}$

Corollary 4.3.7. *There exists a class* **A** *such that classically* $\mathbf{A} = \mathbf{NEXP}$ *but if total non-local correlations are allowed,* $\mathbf{A_{NL}} \subseteq \mathbf{AM}$

Proof. Let $\mathbf{A} = \oplus\mathbf{MIP}[\mathbf{2}](\mathbf{12/16}, \mathbf{11/16} + \epsilon)$ It has been proved by Cleve et al [3] that this class (with classical correlations, one-bit answers) equals $\mathbf{MIP} = \mathbf{NEXP}$. From the discussion above, it results that this class with totally non-local correlations is contained in **AM**. □

The above results are valid for specific subclasses of $\mathbf{MIP_{NL}}$ when the verifier only looks at the XOR of bits. Because the basic non-local transformation we use has this XOR property, we might ask what happens in the general case. We show that $\mathbf{MIP_{NL}}$ is unlikely to be equal to **NEXP**

Theorem 4.3.8. $\mathbf{MIP_{NL}} \in \mathbf{EXP}$

Proof. Let $L \in MIP_{NL}$ and a verifier that decides it. Then, if $r \in L$, there is a set of provers such that the verifier accepts with probability at least c; if $r \notin L$, then for any set of provers, the verifier accepts with probability at most s.

Let x represent questions of the verifier, and y answers of the provers (assume n provers, k rounds). Let $q(x|y)$ be the distribution of the verifier's questions (can be computed efficiently by a polynomial time machine). Let $a(y|x)$ the the distribution of the provers' answers. The acceptance probability of the verifier is:

$$S = \sum_{x,y} q(x|y)a(y|x)Pr[Vaccepts|x, y] \tag{4.1}$$

The goal of the provers is to maximize the acceptance probability of the verifier, so in order to simulate the behavior of the provers we have to be able to approximate $\max_{a(y|x)} S$ and decide if it's greater than c or less than s.

We can think of x as $x = x_{11}...x_{1n}...x_{21}...x_{2n}...x_{k1}...x_{kn}$, where x_{ij} is the question sent to prover j in round i (and we can write y similarly)

The non-local conditions can be written as: for any answer y_{ij} of the provers, its distribution depends only on $x_{i'j}$, with $i' \leq i$ (the questions sent to the same prover in the previous rounds). Mathematically, this can be written as:

$$\forall ij: \ fix\ x_{1j}...x_{ij}, y_{ij}\ then\ \sum_{y} a(y|x) = same\ \forall x \tag{4.2}$$

Normalization conditions: for any input, the probability of obtaining an output is 1.

$$fix\ x\ then\ \sum_y a(y|x) = 1 \tag{4.3}$$

We can think of approximating the acceptance probability of the verifier as the solution to the system:

$$\max_{a(y|x)} \sum_{x,y} q(x|y)a(y|x)Pr[Vaccepts|x,y] \tag{4.4}$$

$$\forall ij:\ fix\ x_{1j}...x_{ij}, y_{ij}\ then\ \sum_y a(y|x) = same\ \forall x \tag{4.5}$$

$$\forall x \sum_y a(y|x) = 1 \tag{4.6}$$

This is a linear program in variables $a(y|x)$ that can be solved in time polynomial in the number of variables and hence exponential in the input size (we only need an approximation of the optimum within an additive factor of $(c-s)/2$)

□

4.4 Quantum correlations

Quantum correlations (entanglement) are a proper subset of the total non-local correlations. It can be proved that, in the case of Alice and Bob game we introduced in the previous section, the best they can do using entanglement is approx. 0.857, whereas with total non-locality the probability is 1. This makes the proof above fail.

However, if we allow promise problems, then it turns out that there is a correlation that is satisfied with probability 1 quantumly, but with probability less than 1 classically. Mathematically, this reduces to:

Claim 4.4.1. *We have a quantum non-signaling (no communication) box that on inputs x, y, and $x \oplus y$ returns a, b, and c such that $a \oplus b \oplus c = xy \oplus x \oplus y$*

Proof. Consider the GHZ state $(|000> + |111>)/\sqrt{2}$ We have three parties, Alice, Bob, and Carol, each one receiving one bit and outputting another one. If the input bit is 0, they measure in the X basis, and if the input bit is 1 they measure in the Y basis. If the result is along +X (+Y) they output 0, otherwise (along -X/-Y) they output 1.

We only have four possible inputs: 000, 011, 101, 110. It's easy to see that for 000 the XOR of the output bits is 0, whereas for the other possible inputs, the XOR of the output bits is 1, which is exactly $xy \oplus x \oplus y$ □

Claim 4.4.2. *If we have a non-signaling box that on inputs x, y, and $x \oplus y$ returns a, b, and c such that $a \oplus b \oplus c = xy \oplus x \oplus y$, we can construct a non-signaling box such that $a' \oplus b' \oplus c' = xy$*

Proof. Let $a' = a \oplus x$, $b' = b \oplus y$, $c' = c$ □

Claim 4.4.3. *A set of $2+k$ machines (provers) that don't communicate but have access to quantum non-local correlations, on input $q_1, q_2, \pi_1, ...\pi_k$ can output bits $b_1, ..., b_{2+k}$ such that $b_1 \oplus ...b_{2+k}$ can define any Boolean function f on q_1, q_2 (k is the number of monomials in f that depend on both q_1 and q_2) Here, π represents the XOR of the two products of variables that come from the two questions q_i in a given monomial (e.g. for monomial $x_1y_1y_2$, the corresponding π is $x_1 \oplus y_1y_2$)*

Proof. Using Claims 2&13 above, each prover can obtain sets a_i for each monomial, then each prover XORs its a's and outputs the answer. □

Definition 4.4.1. Let $\oplus$**MIP[2]** be a class similar to **MIP[2]**, except that the verifier doesn't look at individual prover answers in a given round, but only at the bit-wise XOR (and moreover, answers are one-bit long)

Definition 4.4.2. Let $\oplus$**GHMIP[2]** be similar to $\oplus$**MIP[2]** except that we have a governor G and helpers H_j. The communication with the provers is the same. The verifier sends all questions to the governor which in turns sends to each helper a π_j as defined above (the XOR of the two products of variables that come from the two questions q_i in a given monomial) Each helper returns a bit, then the governor takes the XOR of those bits and returns the answer to the verifier, which takes the XOR of this bit and the provers' answers. Please note that the behavior of the governor is fixed.

Theorem 4.4.3. *For any verifier $V_\oplus$ and any 1-round protocol involving 2 communicating provers P_i^{COMM}, there is a set of quantum non-local provers P_i^Q such that the acceptance probability is the same.*

Proof. We'll prove that there is a set P_i^Q that for each given questions $q_1...q_n$ to the provers, give the same behavior of the verifier.

Consider the $(V_\oplus, P_i^{COMM})$ protocol. The provers return the answers r_1, r_2 that maximize the acceptance probability of the verifier. Let b be the bit-wise XOR of these answers (the only thing that counts from the point of view of the verifier) b is a Boolean function of the questions, and hence simulated by a set of quantum non-local provers + governor + helpers (as per Claim 14). So, there is a set of quantum non-local provers that can create the same b and that would make the verifier accept with the same probability. □

Theorem 4.4.4. $\oplus$**MIP**$[2]_{\mathbf{COMM}} = \oplus$**GHMIP**$[2]_{\mathbf{Q}}$

Proof. $L \in \oplus$**MIP**$[2]_{\mathbf{COMM}}$ iff $\exists V_\oplus$ such that:

- $x \in L \Rightarrow \exists P_i^{COMM}$ such that $\Pr[(V_\oplus, P_i^{COMM})$ acc.$] \geq c$
- $x \notin L \Rightarrow \forall P_i^{COMM}$ $\Pr[(V_\oplus, P_i^{COMM})$ acc.$] \leq s$

$L \in \oplus\mathbf{GHMIP}[\mathbf{2}]_{\mathbf{Q}}$ iff $\exists V'_{\oplus}$ such that:

- $x \in L \Rightarrow \exists P_i^Q$ such that $\Pr[(V'_{\oplus}, P_i^Q) \text{ acc.}] \geq c$
- $x \notin L \Rightarrow \forall P_i^Q \Pr[(V'_{\oplus}, P_i^Q) \text{ acc.}] \leq s$

" =>": Let $V'_{\oplus} = V_{\oplus}$

Let $x \in L \in \oplus\mathbf{MIP}[\mathbf{2}]_{\mathbf{COMM}}$ Then $\exists P_i^{COMM}$ such that $\Pr[(V_{\oplus}, P_i^{COMM}) \text{ acc.}] \geq c$. Using Theorem 17, we obtain that $\exists P_i^Q$ such that $\Pr[(V_{\oplus}, P_i^Q) \text{ acc.}] \geq c$

Let $x \notin L \in \oplus\mathbf{MIP}[\mathbf{2}]_{\mathbf{COMM}}$ Then $\forall P_i^{COMM} \Pr[(V_{\oplus}, P_i^{COMM}) \text{ acc.}] \leq s \Rightarrow \forall P_i^Q \Pr[(V_{\oplus}, P_i^Q) \text{ acc.}] \leq s$

" <=": Let $V'_{\oplus} = V_{\oplus}$

Let $x \in L \in \oplus\mathbf{GHMIP}[\mathbf{2}]_{\mathbf{Q}}$ Then $\exists P_i^Q$ such that $\Pr[(V_{\oplus}, P_i^Q) \text{ acc.}] \geq c \Rightarrow \exists P_i^{COMM}$ such that $\Pr[(V_{\oplus}, P_i^{COMM}) \text{ acc.}] \geq c$

Let $x \notin L \in \oplus\mathbf{GHMIP}[\mathbf{2}]_{\mathbf{Q}}$ Then $\forall P_i^Q \Pr[(V_{\oplus}, P_i^Q) \text{ acc.}] \leq s$ Suppose $\exists P_i^{COMM}$ such that $\Pr[(V_{\oplus}, P_i^{COMM}) \text{ acc.}] > s$ Using Theorem 17, we obtain that $\exists P_i^Q$ such that $\Pr[(V_{\oplus}, P_i^Q) \text{ acc.}] > s$, contradiction. So, $\forall P_i^{COMM} \Pr[(V_{\oplus}, P_i^{COMM}) \text{ acc.}] \leq s$ □

Theorem 4.4.5. $\oplus\mathbf{MIP}[\mathbf{2}]_{\mathbf{COMM}} \subseteq \mathbf{AM}$

Proof. $L \in \mathbf{AM}$ iff $\exists V$ (using just one round) such that:

- if $x \in L$ then $\exists P$ such that $\Pr[(V, P) \text{ acc}] \geq c$
- if $x \notin L$, then $\forall P$, $\Pr[(V, P) \text{ acc}] \leq s$

Let V' the **AM** verifier be such that it is identical to the $\oplus\mathbf{MIP}[\mathbf{2}]_{\mathbf{COMM}}$ verifier after it computes the XOR of the provers' answers (and asks all questions to the only prover)

Let $x \in L \in \oplus\mathbf{MIP}[\mathbf{2}]_{\mathbf{COMM}}$ Then $\exists P_i^{COMM}$ such that $\Pr[(V, P_i^{COMM}) \text{ acc.}] \geq c$. Let P simulate the behavior of P_i^{COMM} We have: $\Pr[(V', P) \text{ acc}] \geq c$

Let $x \notin L \in \oplus\mathbf{MIP}[\mathbf{2}]_{\mathbf{COMM}}$ Then $\forall P_i^{COMM} \Pr[(V, P_i^{COMM}) \text{ acc.}] \leq s$ Suppose $\exists P$ such that $\Pr[(V', P) \text{ acc}] \geq s$. But P could be simulated by P_i^{COMM}, contradiction. □

Corollary 4.4.6. $\oplus\mathbf{GHMIP}[\mathbf{2}]_{\mathbf{Q}} \subseteq \mathbf{AM}$

Theorem 4.4.7. $\oplus\mathbf{GHMIP}[\mathbf{2}] = \oplus\mathbf{MIP}[\mathbf{2}]$

Proof. Clearly, any $\oplus\mathbf{MIP}[\mathbf{2}]$ protocol can be simulated by a $\oplus\mathbf{GHMIP}[\mathbf{2}]$ machine with the same acceptance probability. We only have to prove the converse. Each of the helper's answers is a (linear) function of $p_1 + p_2$, where p_1 is a product of variables from q_1 and p_2 is a product of variables from q_2 (q represent the questions to the provers). The governor's answer is the XOR of the helpers' answers, hence also a (linear) function in p_{1i} and p_{2i}. Now, because the verifier only looks at the XOR of the provers' and governor's answers, we can define a new set of provers that XORs the corresponding linear part that depends on p_{1i} (from prover 1) and p_{2i} (from prover 2) respectively to its answer - and not use the governor and helpers anymore. Hence, any $\oplus\mathbf{GHMIP}[\mathbf{2}]$ protocol can be simulated by a $\oplus\mathbf{MIP}[\mathbf{2}]$ protocol with the same acceptance probability □

Corollary 4.4.8. *There exists a class* $\mathbf{A}$ *such that* $\mathbf{A_C} = \mathbf{NEXP}$ *and* $\mathbf{A_Q} \subseteq \mathbf{AM}$

Proof. Let $\mathbf{A} = \oplus\mathbf{GHMIP}[\mathbf{2}](\mathbf{12/16}, \mathbf{11/16} + \epsilon)$ This class (with classical correlations, one-bit answers) equals $\oplus\mathbf{MIP}[\mathbf{2}](\mathbf{12/16}, \mathbf{11/16} + \epsilon)$ which (proved by Cleve et al) equals $\mathbf{MIP_C} = \mathbf{NEXP}$. From the discussion above, it results that this class with quantum correlations is in $\mathbf{AM}$. □

We can modify the behavior of the governor such that a claim similar to Claim 3 would hold in the quantum case. In that case, the resulting class would be equal to PSPACE, while the same class with no correlations would be equal to NEXP. We must emphasize again that all these classes are artificial constructions and the governor has a fixed behavior.

Chapter 5

Conclusions

In this study we presented several results that bring out different aspects of correlations naturally arising (quantum) or theoretically possible (general non-local) among two or more parties. In particular, we looked at several interactive games and proof systems (Magic Square, 3SAT, MIP and MIP variants) and showed that under different protocols, correlations can weaken them in various degrees.

We first focused our attention on two particular games: Magic Square, and 3SAT. For both games, drawing on the monogamy of entanglement principle, we showed that by adding an extra prover, no cheating strategies are allowed. We then generalized the results for Magic Square and 3SAT by looking at non-commuting provers, a superset of entangled provers (communication is allowed, but operators applied by different provers must commute). Using this method, we obtained a generalized Tsirelson inequality that we applied to the Magic Square. Hence, we were able to give provably optimal strategies for the general Magic Square with n players. We also recovered a similar result for 3SAT as with entangled provers, and we also improved on it by showing that the gap is inverse exponential in the input size.

We then argued that general non-local correlations lead to several class collapses: classes that are strong when classical correlations are allowed, become weak when provers have access to general non-local correlations. In particular, there are classes that classically are equal to **NEXP**, but collapse to **AM** once such correlations are allowed. We also showed that **MIP** where the verifier only looks at the XOR of the answers collapses to **PSPACE**. By writing general non-local correlations as linear constraints, **MIP** collapses to **EXP** under such correlations (vs being equal to **NEXP** classically). Finally, we presented an artificial **MIP**-like class built on a promise problem, that classically is equal to **NEXP**, but that also collapses to **AM** when quantum correlations are present.

We would like to have a better understanding of the power of the interactive proofs under different types of correlations. In particular, we would like to have matching upper and lower bounds for **MIP**. Recent work by Ito [20] showed that **MIP** with general non-local correlations with 2 provers, one round is contained in **PSPACE**. Combining this result with work by Ito, Kobayashi and Matsumoto [21] exactly characterizes **MIP** with non-local correlations with 2 provers, one round as

equal to **PSPACE**. An open question is whether this equality holds if we add more provers or increase the number of rounds. In the case of quantum correlations, we know that if the amount of entanglement is limited, then quantum correlations don't help [28], and that in the particular case of XOR games the quantum-to-classical gap is small [13]. Although we know that by adding extra provers they cannot cheat perfectly, it would be interesting to find more general classes of interactive games for which the quantum-to-classical gap is small, in addition to XOR games.

Another direction of interesting research is trying to understand the gap between quantum and general non-local correlations. In a sense, we would like to know what makes a correlation general, and whether there is something particularly interesting about how much we can simulate PR boxes with different types of correlations. Brassard et all [7] showed that using amplification, PR boxes that have a 0.908 or better reliability can be used to simulate a box with almost perfect reliability. We also know that quantum PR boxes have a 0.854 reliability, and hence cannot simulate perfect PR boxes. It would be interesting to bridge the gap between quantum and the PR boxes that can simulate perfect correlations.

Answers to some of those questions would help us better understand not only various protocols used in interactive games, but also the nature and power of correlations naturally arising in quantum mechanics.

Bibliography

[1] P. K. Aravind. The magic squares and bell theorem. *arXiv.org e-Print quant-ph/0206070*, 2002.

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

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

[4] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Non-local correlations as an information theoretic resource. *quant-ph/0404097*, 2004.

[5] Jonathan Barrett and Stefano Pironio. Popescu–Rohrlich correlations as a unit of nonlocality. *Physical Review Letters*, 95(140401), September 2005. arXiv:quant-ph/0506180v2.

[6] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi 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, May 1988.

[7] G. Brassard, H. Buhrman, N Linden, A. A. Methot, A. Tapp, and F. Unger. A limit on nonlocality in any world in which communication complexity is not trivial. *arXiv:quant-ph/0508042*.

[8] H. Buhrman and S. Massar. Causality and tsirelson bounds. *quant-ph/0409066*.

[9] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable thoeries. *Physical Review Letters, 23(15)*, pages 800–884, 1969.

[10] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, October 1969.

[11] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. *Proc. 19th IEEE Conference on Computational Complexity*, pages 236–249, 2004.

[12] Richard Cleve, Dmitry Gavinsky, and Rahul Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive PIRs. *Quantum Information and Computation*, 9(7–8):648–656, July 2009. Manuscript at arXiv:0707.1729v1 [quant-ph].

[13] Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings: Nineteenth Annual IEEE Conference on Computational Complexity (CCC 2004)*, pages 236–249, June 2004. arXiv:quant-ph/0404076v1.

[14] Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *Proceedings: Twenty-Third Annual IEEE Conference on Compuational Complexity (CCC 2008)*, pages 199–210, June 2008. arXiv:0803.4373v1 [quant-ph].

[15] Ding-Zhu Du and Ker-I Ko. *Theory of Computational Complexity*. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 2000.

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

[17] Uriel Feige and László 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, May 1992.

[18] Lance Fortnow, John Rompel, and Michael Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134(2):545–557, November 1994.

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

[20] T. Ito. No-signaling provers can be approximated in polynomial space. *Personal communication*.

[21] T. Ito, H. Kobayashi, and K. Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. *arXiv:quant-ph/0810.0693*.

[22] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proceedings: Twenty-Fourth Annual IEEE Conference on Compuational Complexity (CCC 2009)*, pages 217–228, July 2009.

[23] J. Kempe and T. Vidick. On the power of entangled quantum provers. *arXiv.org e-Print quant-ph/0612063*, 2006.

[24] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. arXiv:0704.2903v2 [quant-ph], November 2007.

[25] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. In *Proceedings: Forty-Ninth Annual IEEE Symposium on Foundations of Computer Science (FOCS 2008)*, pages 447–456, October 2008.

[26] H. Kobayashi and K. Matsumoto. Simulating mip(2,1) protocols by mip*(3,1), and ip protocols by mip*(2,1). *Personal communication*.

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

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

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

[30] N. D. Mermin. Hidden variables and the two theorems of john bell. *Reviews of Modern Physics 65(3)*, pages 803–815, 1993.

[31] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(073013), July 2008. arXiv:0803.4290v1 [quant-ph].

[32] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2001.

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

[34] S. Popescu and D. Rohrlich. Nonlocality as an axiom. *Foundations of Physics*, 1994.

[35] Xiaoming Sun, Andrew Chi-Chih Yao, and Daniel Preda. On entangled quantum 3-prover systems for SAT and the magic square, 2007. Invited talk at QIP 2007 presented by A. Yao.

[36] B. Toner. A proof system for np with entangled provers. *Personal communication*.

[37] B. Toner. Monogamy of nonlocal quantum correlations. *arXiv.org e-Print quant-ph/0601172*, 2006.

[38] B. S. Tsirelson. Quantum generalizations of bell inequality. *Letters in Mathematical Physics, 4(2)*, pages 93–100, 1980.

[39] B. S. Tsirelson. Quantum analogues of the bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics, 36*, pages 557–570, 1987.

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

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

[42] W. van Dam. Nonlocality and communication complexity. *D.Phil. Thesis, University of Oxford*, 2000.

[43] S. Wehner. *quant-ph/0508201*.

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