CS682A: Paper Report
Prof. Rajat Mittal

December 2, 2022

Consequences and Limits of Nonlocal Strategies

Richard Cleve, Peter Hoyer, Ben Toner, John Watrous

Ayush Kumar (190213)
Niket Jain (190547)
Gurbaaz Singh Nandra (190349)

1 Background of the Problem & Context

A *non-local game* is a hypothetical cooperative game that is played by 2 or more players against a referee, where the goal of players is to jointly win the game. The only communication allowed is between the players and the referee, where each player receives a random question from a known probability distribution and responds with an answer to the referee. Finally, the referee collects the answers, and based on the answers to the questions, decides if the players won or not. The figure below provides an idea of the flow of a non-local game consisting of a referee and two players, say *Alice* and *Bob*.

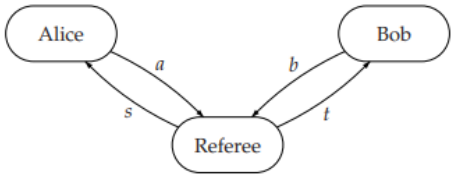

Figure 1: The communication structure of a non-local game

1.1 Mathematical Formulation

A non-local game G is defined as $G = G(V, \pi)$, where π is the probability distribution on the question set $S \times T$, and V is a predicate on $S \times T \times A \times B$. A pair of questions (s, t) from $(S \times T)$ is chosen from the distribution by the referee, and pair of answers (a, b) from $(A \times B)$ is sent by Alice and Bob. The game is won by players Alice and Bob if the predicate V evaluates to *true*, or else it is lost. The predicate V is often denoted by $(a, b \mid s, t)$ rather than (s, t, a, b) to highlight the conditional dependence of answers (a, b) on given questions (s, t).

1.2 Classical Value of a Non-Local Game

Game value is defined as the maximum probability with which Alice and Bob can win a game G, and is denoted using $\omega_x(G)$. This is always obtained by some deterministic strategy, given that any probabilistic strategy can be expressed as a convex combination of deterministic strategies. Thus,

$$\omega_c(G(V, \pi)) = \max_{a,b} \sum_{s,t} \pi(s, t) V(a(s), b(t) | s, t) \tag{1}$$

where the maximum is over all the functions $a : S \to A$ and $b : T \to B$ Note that a deterministic strategy is a restricted type of classical strategy where a and b are simply functions of s and t, respectively.

1.3 Introduction to Quantum Strategies

The most important part of the quantum strategies for any non-local game is the presence of an *entangled* shared state ($|\psi\rangle$) by 2 players in the beginning. The strategy is that on receiving some set of input (s, t), Alice performs measurement corresponding to her input, s and gets output a. Bob gets output b in a similar way. Mathematically, $|\psi\rangle \in A \otimes B$, where A represents Alice's space and B represents Bob's.

We also need two collections of positive semi-definite matrices $\{X_s^a : s \in S, a \in A\}$, $\{Y_t^b : t \in T, b \in B\}$ satisfying $\sum_(a \in A) X_s^a = 1$ and $\sum_(b \in B) Y_t^b = 1 \forall s \; in S; \; t \in T$. Here, this collection $\{X_s^a : a \in A\}$ describes the measurement performed by Alice whenever she receives the question s, and likewise for Bob. The probability that Alice answers with a and Bob with b when input is $\{s, t\}$ is given by the expression -

$$\langle \psi | X_s^a \otimes Y_t^b | \psi \rangle \tag{2}$$

Therefore, the probability of winning the game using quantum strategy is given by -

$$\sum_{(s,t) \in S \times T} \pi_{(s,t)} \sum_{(a,b) \in A \times B} \langle \psi | X_s^a \otimes Y_t^b | \psi \rangle V(a, b | s, t) \tag{3}$$

where $\pi_{(s,t)}$ denotes the probability of occurrence of input (s, t). The *quantum value* of a game, denoted by $w_q(G)$ is the supremum of winning probabilities of over all the quantum strategies of Alice and Bob. We measure the outcomes using *observables*, which are basically Hermitian matrices with real eigenvalues.

2 Problem Background

2.1 Examples of Non Local Games violating Bell inequalities

In quantum information theory, a Bell [2] inequality is analogous to an upper bound on the probability with which Alice and Bob can win a non-local game using a classical strategy, and quantum strategies that beat these bounds (i.e. game value would be higher than the classical game value) are said to violate a Bell inequality. The paper presents several instances of non-local games where quantum strategies outperform classical strategies -

2.1.1 The CHSH game [3]

The mathematical formulation of this game is as follows:-

Let $S = T = A = B = \{0, 1\}$, let π be the uniform distribution on $S \times T$, and let V be the predicate

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

One can see that there is no way to win the game perfectly, and the best classical strategy of choosing $a = b = 0$ gives a winning probability of $3/4$ (thus $\omega_c(G) = 3/4$).

However there exists a quantum strategy that gives a better winning probability than $3/4$, and the quantum value of the game $\omega_q(G) = \cos^2(\pi/8) \approx 0.85$.

2.1.2 The Magic Square game [11] [8] [9]

This is a game where there is no *perfect* classical strategy, but there exists a perfect quantum strategy, i.e. one which ensures a winning probability of 1. In this game, Alice is asked to fill in the values in either a row or a column of a binary matrix (randomly selected) and Bob is asked to fill in a single entry of the matrix, that is randomly chosen among the three entries given to Alice. The requirement is that the values given by Alice must have even parity for row and odd for column and that Bob's answer is consistent with Alice's.

One can see that the classical value of this game cannot be 1, based on the fact that there does not exist a 3×3 binary matrix with the property that each row has even parity and each column has odd parity. The best classical strategy ensures a winning probability of $17/18$. However, there exists a perfect quantum strategy for this game, meaning that the strategy wins with probability 1.

Through the above 2 examples, we can see that through the use of entanglement, it is indeed possible to outperform classical strategies for non-local games. This happens because of the entangled state Alice and Bob share. Alice measures her part of the state in a way that depends on her input s and gets her answer satisfying the required condition. Alice's action *modifies* the state on Bob's side, and his measurement which depends on t is defined in a way that tries to satisfy the requirements of the game, thus resulting in better performance.

2.2 Multi Prover Interactive Systems

Non-local games are seen as a natural abstraction of multi-prover interactive proof systems. These systems provide an abstract machine that models computation as the exchange of messages between two parties: a prover and a verifier to ascertain whether a given string belongs to a language or not. It is assumed that the prover possesses unlimited computational resources but cannot be trusted, while the verifier has bounded computation power but is assumed to be always honest.

It is logical to take into account prover techniques that include communicating entangled quantum information before the proof system is executed because the interactive proof system paradigm is designed to limit the capabilities of the verifier rather than the prover(s).

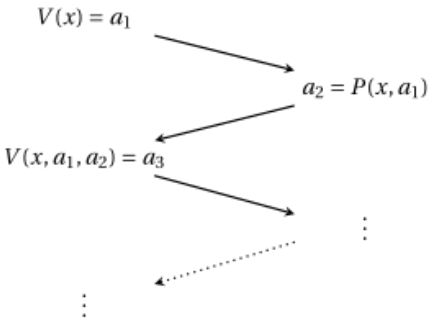

Figure 2: General representation of an interactive proof protocol

So the question then becomes, what happens when the provers can employ quantum strategies? No changes are made to the verifier, who remains classical, and all communication between the verifier and the provers remains classical.

The same idea is employed and the interaction is restricted to two stages: a query stage where the verifier sends information to the provers, and a response stage where the provers send information to the verifier. One can associate a nonlocal game G_x to each string x with the property that $\forall$ yes-inputs x, $w_q(G_x)$ is close to 1, else $w_q(G_x)$ is close to 0. The paper presents two examples of natural two-prover one-round proof systems that are classically sound, but become unsound when the provers use quantum strategies:

2.2.1 Graph Coloring Proof System

It is possible to think of the Odd Cycle game as a protocol where two provers are competing to persuade a verifier that a specific graph is two-colorable. This concept is generalizable to any graph G and k colors. The verifier asks each prover for the color of a vertex (from a possible set of k), and it stipulates that the colors must match whenever the provers receive neighboring vertices and differ when they receive the same vertex. If G is k-colorable, then the provers can answer based on a valid coloring. If not, there must be some inconsistency for some (s,t) and so the value of the game cannot be 1. The verifier can amplify the difference by repeating this game a polynomial number of times between the 2 cases: colorable or not. This proof system breaks down in case of entangled provers. There exists a sequence of graphs G_n such that:

1. For any n, there is a perfect quantum strategy for the Graph Coloring proof system with graph G_n and $k = n$ colors.
2. For sufficiently large n, G_n is not k-colorable.

2.2.2 3 SAT Proof System

We consider a non local game G_f involving Alice and Bob, where Alice is provided with a clause and Bob is given a variable from the clause. Alice needs to provide a valid assignment for the clause, satisfying the clause, while Bob needs to provide an assignment for the variable satisfying Alice's choice. In Mathematical terms, let the variables be $x_0, x_1, \ldots, x_{n-1}$ and the clauses be $c_0, c_1, ...c_{m-1}$. Then, $S = Z_m, T = Z_n, A = \{0,1\}^3, B = \{0,1\}$. The predicate $V(a,b|s,t)$ takes value 1 *iff* Alice's assignment for the variables in c_s satisfies c_s & is consistent with assignment $x_t = b$. If f is satisfiable then, $w_c(G_f) = 1$. If f is unsatisfiable, then $w_c(G_f) < 1 - 1/3m$ as out of all $3m$ possibilities, atleast 1 would violate the clause. However a simple counterexample can be derived based on the Magic Square game, where f is unsatisfiable, but there is a perfect quantum strategy for the above two prover proof system.

We consider 9 boolean variables for this Magic Square game, $x_{00}, x_{01}, x_{02}, x_{10}, x_{11}, x_{12}, x_{20}, x_{21}$ and x_{22}. They represent a 3×3 boolean matrix. There are 6 parity conditions in the magic square game, each row has even parity & each column has odd parity & each condition can be expressed with 4 clauses:-

$$(\overline{x_{00}} \vee \overline{x_{01}} \vee \overline{x_{02}}) \wedge (\overline{x_{00}} \vee x_{01} \vee x_{02}) \wedge (x_{00} \vee \overline{x_{01}} \vee x_{02}) \wedge (x_{00} \vee x_{01} \vee \overline{x_{02}}) \tag{4}$$

Thus we would have 24 such clauses. This clause is satisfied only when $x_{00} \oplus x_{01} \oplus x_{02} = 0$. Thus, as we know, this formula is unsatisfiable, but since we have the perfect strategy for the Magic Square game, the quantum strategy defeats this 3 SAT game with certainty.

3 Results and Proof Techniques

3.1 Theorem 1

Let G be a binary game. If there exists a quantum strategy for G that wins with probability 1, then $w_c(G) = 1$.
Proof :- Assume that a perfect quantum strategy for G is given. More specifically, we assume that this strategy uses a shared entangled state $|\psi\rangle$, and that Alice and Bob's measurements are projective measurements on A and B, respectively, making it possible to describe their measurements using ±1 observables, $A_s \& B_t$. Thus, the probability that Alice and Bob respond to (s, t) with $(\alpha, \beta) \in \{1, -1\} \times \{1, -1\}$ is

$$q(\alpha, \beta \mid s, t) = \frac{1}{4} \langle\psi| (\mathbb{1} + \alpha A_s) \otimes (\mathbb{1} + \beta B_t) |\psi\rangle = \frac{1}{4} + \frac{\alpha}{4} \langle\psi| A_s \otimes \mathbb{1} |\psi\rangle + \frac{\beta}{4} \langle\psi| \mathbb{1} \otimes B_t |\psi\rangle + \frac{\alpha\beta}{4} \langle\psi| A_s \otimes B_t |\psi\rangle .$$

To Prove these we use the facts that $X_s^1 + X_s^{-1} = \mathbb{1}$ and $X_s^1 - X_s^{-1} = A_s$. Similarly, $Y_t^1 + Y_t^{-1} = \mathbb{1}$ and $Y_t^1 - Y_t^{-1} = B_t$.

We will now define functions $a : S \to \{+1, -1\}$ and $b : T \to \{+1, -1\}$ that represent a perfect deterministic strategy for Alice and Bob. First, fix an orthonormal basis $\{|\phi_1\rangle, \ldots, |\phi_{n^2}\rangle\}$ of $\mathcal{A} \otimes \mathcal{B}$ such that $|\phi_1\rangle = |\psi\rangle$ and where $|\phi_2\rangle, \ldots, |\phi_{n^2}\rangle$ are chosen arbitrarily (subject to the constraint of orthonormality). Next, define functions $k : S \to \{1, \ldots, n^2\}$ and $\ell : T \to \{1, \ldots, n^2\}$ as

$$k(s) = \min \left\{ j \in \{1, \ldots, n^2\} : \langle\phi_j| A_s \otimes \mathbb{1} |\psi\rangle \neq 0 \right\}$$
$$\ell(t) = \min \left\{ j \in \{1, \ldots, n^2\} : \langle\phi_j| \mathbb{1} \otimes B_t |\psi\rangle \neq 0 \right\}$$

and also define a function $\kappa : C]\{0\} \to \{+1, -1\}$ over the nonzero complex numbers as

$$\kappa(z) = \begin{cases} +1 & \text{if } \arg(z) \in [0, \pi) \\ -1 & \text{if } \arg(z) \in [\pi, 2\pi). \end{cases}$$

Finally, define :- $\quad a(s) = \kappa\left(\langle\phi_{k(s)}| A_s \otimes \mathbb{1} |\psi\rangle\right) \quad$ and $\quad b(t) = \kappa\left(\langle\phi_{\ell(t)}| \mathbb{1} \otimes B_t |\psi\rangle\right)$.

We will now prove that the functions a and b define a perfect deterministic strategy for G, so that $\omega_c(G) = 1$.

To do this, we prove that every question pair (s, t) is answered with $(a(s), b(t))$ by the given quantum strategy with a positive probability: $q(a(s), b(t) \mid s, t) > 0$. Given that the quantum strategy is perfect, it follows that $(a(s), b(t))$ is correct for (s, t) whenever $\pi(s, t) > 0$.
To prove that $q(a(s), b(t) \mid s, t) > 0$ for every choice of s and t, we first observe the following two facts:

1. if $\langle\psi| A_s \otimes \mathbb{1} |\psi\rangle \neq 0$, then $a(s) \langle\psi| A_s \otimes \mathbb{1} |\psi\rangle > 0$
   (since $\langle\psi| A_s \otimes \mathbb{1} |\psi\rangle$ is real, & if it's $\neq 0$ we have $k(s) = 1$, so that $a(s) = \text{sign}\left(\langle\psi| A_s \otimes \mathbb{1} |\psi\rangle\right)$)
2. if $\langle\psi| \mathbb{1} \otimes B_t |\psi\rangle \neq 0$, then $b(t) \langle\psi| \mathbb{1} \otimes B_t |\psi\rangle > 0$.
   (if one or both among $\langle\psi| A_s \otimes \mathbb{1} |\psi\rangle$ or $\langle\psi| \mathbb{1} \otimes B_t |\psi\rangle$ is nonzero, then $a(s) \langle\psi| A_s \otimes \mathbb{1} |\psi\rangle + b(t) \langle\psi| \mathbb{1} \otimes B_t |\psi\rangle > 0$.)

As $\langle\psi| A_s \otimes B_t |\psi\rangle \geq -1$, it follows that

$$q(a(s), b(t) \mid s, t) = \frac{1}{4} + \frac{a(s)}{4} \langle\psi| A_s \otimes \mathbb{1} |\psi\rangle + \frac{b(t)}{4} \langle\psi| \mathbb{1} \otimes B_t |\psi\rangle + \frac{a(s)b(t)}{4} \langle\psi| A_s \otimes B_t |\psi\rangle > 0.$$

The quantum strategy therefore results in the answers $(a(s), b(t))$ to the question pair (s, t) with a nonzero probability.

The remaining case to consider is that $\langle\psi| A_s \otimes \mathbb{1} |\psi\rangle = \langle\psi| \mathbb{1} \otimes B_t |\psi\rangle = 0$. In this case we have

$$q(a(s), b(t) \mid s, t) = \frac{1}{4} + \frac{a(s)b(t)}{4} \langle\psi| A_s \otimes B_t |\psi\rangle .$$

As in the first case, we wish to prove that q(a(s), b(t)|s, t) is positive, so we assume toward contradiction that q(a(s), b(t)|s, t) = 0, which means that $a(s)b(t) \langle\psi| A_s \otimes B_t |\psi\rangle$ = -1. We have that

$$a(s)b(t) \langle\psi| A_s \otimes B_t |\psi\rangle = \sum_{j=1}^{n^2} a(s)b(t) \left\langle\psi| A_s \otimes \mathbb{1} |\phi_j\right\rangle \left\langle\phi_j| \mathbb{1} \otimes B_t |\psi\right\rangle$$

We observe that this quantity corresponds to the inner product of the two n^2 dimensional unit vectors whose j-th entries are given by $a(s) \left\langle\psi| A_s \otimes \mathbb{1} |\phi_j\right\rangle$ and $b(t) \left\langle\phi_j| \mathbb{1} \otimes B_t |\psi\right\rangle$. if this inner pdt is -1, one must be the negation of the other for every choice of $j = 1, \ldots, n^2$. If $k(s) \neq l(t)$, then this condition wouldn't hold for $j = \min\{k(s), l(t)\}$, also if $k(s) = l(t)$, then for $j = k(s)$, we find that *arg* for both $a(s) \left\langle\psi| A_s \otimes \mathbb{1} |\phi_j\right\rangle$ and $b(t) \left\langle\phi_j| \mathbb{1} \otimes B_t |\psi\right\rangle$ are in the range $[0, \pi)$ and thus the condition again fails to hold, giving a contradiction and hence proving the result.

3.2 Theorem 2 (Tsirelson) [7]

Let S and T be finite, nonempty sets, and let $\{c_{s,t} : (s,t) \in S \times T\}$ be a collection of real numbers in the range $[-1,1]$. Then the following are equivalent:

1. *There exists a positive integer n, complex Hillert spaces $\mathcal{A}$ and $\mathcal{B}$ with finite dimension n, a anit vector $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$, a collection $\{A_s : s \in S\}$ of ± 1 obseroables on $\mathcal{A}$, and a collection $\{B_t : t \in T\}$ of ± 1 observables on $\mathcal{B}$, such that*

$$\langle \psi | A_s \otimes B_t | \psi \rangle = c_{s,t}$$

   for all $(s,t) \in S \times T$.

2. *There exists a positive integer m and two collections $\{|u_s\rangle : s \in S\}$ and $\{|v_t\rangle : t \in T\}$ of unit vectors in $\mathbf{R}^m$ such that*

$$\langle u_s \mid v_t \rangle = c_{s,t}$$

   for all $(s,t) \in S \times T$.

Moreover, if the first item holds for a fixed choice of n, then the second holds for $m = 2n^2$; and if the second item holds for a fixed choice of m, then the first holds for $n = 2^{\lfloor m/2 \rfloor}$.

Advantage over the trivial strategy

Next, to state certain upper bounds on $\omega_q(G)$ for XOR games, it will be helpful to define the trivial random strategy for Alice and Bob as one where they ignore their inputs and answer uniformly generated random bits. If $\tau(G)$ denotes the success probability of game (G, π) when Alice and Bob are restricted to this trivial strategy, then

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

3.3 Proposition 1

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

$$\omega_q(G) - \tau(G) = \frac{1}{2} \max_{\{|u_s\rangle\}\{|p_\ell\rangle\}} \sum_{s,t} \pi(s,t)(V(0 \mid s,t) - V(1 \mid s,t)) \langle u_s \mid v_t \rangle ,$$

where the maximum is over all choices of unit vectors $\{|u_s\rangle : s \in S\} \cup \{|v_t\rangle : t \in T\}$ in $\mathbf{R}^m$.

Proof. Consider any quantum strategy for Alice and Bob given by a shared entangled state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$ and collections of observables $\{A_s : s \in S\}$ and $\{B_1 : t \in T\}$. We associate with each A_s a real unit vector $|u_s\rangle$ and with each B_t a real unit vector $|v_t\rangle$, according to Theorem 2 . On input (s,t), the probability that Alice and Bob's answers are equal is

$$\left\langle \psi \left| X_s^0 Y_t^0 + X_s^1 Y_t^1 \right| \psi \right\rangle = \frac{1}{2} + \frac{1}{2} \langle \psi | A_s \otimes B_t | \psi \rangle = \frac{1}{2} + \frac{1}{2} \langle u_s \mid v_t \rangle$$

It follows that their answers are not equal with probability $(1 - \langle u_s \mid v_t \rangle)/2$. Hence the probability that Alice and Bob win using this strategy is

$$\frac{1}{2} \sum_{s,t,c} \pi(s,t) V(c \mid s,t) + \frac{1}{2} \sum_{s,1} \pi(s,t)(V(0 \mid s,t) - V(1 \mid s,t)) \langle u_s \mid v_t \rangle$$

Assuming the spaces $\mathcal{A}$ and B have dimension n, the vectors $|u_s\rangle$ and $|v_l\rangle$ are unit vectors in $\mathbb{R}^{2u^2}$. Although the dimension n is a priori unbounded, the winning probability depends only on the inner products among the unit vectors $\{|u_s\rangle : s \in S\}$ and $\{|v_t\rangle : t \in T\}$. We may therefore project onto the span of $\{|u_s\rangle : s \in S\} \cup \{|v_t\rangle : t \in T\}$, which is a space with dimension at most $|S| + |T|$. Indeed, it is sufficient to project the vectors $\{|u_s\rangle : s \in S\}$ onto the span of the vectors $\{|v_t\rangle : t \in T\}$ (or vice versa). The dimension of this space is at most $m = \min(|S|, |T|)$. Without loss of generality, let us assume $|S| \leq |T|$. Although the vectors $\{|u_s\rangle : s \in S\}$ will not necessarily remain unit vectors after orthogonal projection, the maximum over all vectors $\left\{|u_s\rangle \in \mathbb{R}^{|T|} : s \in S, \| |u_s\rangle \| \leq 1\right\}$ is achieved by points on the boundary-unit vectors-and so it is sufficient to restrict to this case.

We now show this strategy can be realized as a quantum protocol. The maximization is over a compact set, so the maximum is achieved by some choice of vectors $\{|u_s\rangle : s \in S\}$ and $\{|v_t\rangle : t \in T\}$ in $\mathbb{R}^m$. Let $|\psi\rangle$ be a maximally entangled state on $\lceil m/2 \rceil$ qubits. By Theorem 2 , there are observables $\{A_s\}$ and $\{B_l\}$ such that

$$\langle \psi | A_s \otimes B_t | \psi \rangle = \langle u_s \mid v_l \rangle$$

for all $s \in S$ and $t \in T$. Thus the strategy can be realized as a quantum strategy. The maximization in Proposition 1 can be cast as a semidefinite program, which can be approximated to within an additive error of ε in time polynomial in $|S| + |T|$ and in $\log(1/\varepsilon)$.

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

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

3.4 Upper bound for value of XOR games

The paper gives two bounds for XOR games. The first case is when the success probability of the best classical strategy is not much better than the trivial strategy $\tau(G)$. In this case, no quantum strategy can perform significantly better. The bound has been expressed in terms of the Grothendieck's constant [1] which is defined as:

Grothendieck's constant, K_G is the smallest number such that for all integers $N \geq 2$ and all $N \times N$ real matrices M, if

$$\left| \sum_{s,t} M(s,t) a_s b_t \right| \leq 1$$

for all numbers $a_1, \ldots, a_N, b_1, \ldots, b_N$ in [-1, 1], then

$$\left| \sum_{s,t} M(s,t) \langle u_s | v_t \rangle \right| \leq K_G$$

for all unit vectors $|u_1\rangle, \ldots, |u_N\rangle, |v_1\rangle, \ldots, |v_N\rangle$ in $\mathbb{R}^n$ (for any choice of n).
It is known that $1.6769 \leq K_G \leq 1.7822$ (upper bound established by Krivine [4] and lower bound by Davie [5])

The paper shows that if G is an XOR game, then

$$\omega_q(G) - \tau(G) \leq K_G |\omega_c(G) - \tau(G)|$$

The result can be proved by defining a matrix M which satisfies the first inequality in the definition of the constant. The proof is as follows:

Suppose, without loss of generality, that $|S| = |T| = N$. Define an $N \times N$ matrix M by

$$M(s,t) = \frac{1}{2[\omega_c(G) - \tau(G)]} \pi(s,t)[V(0|s,t) - V(1|s,t)]$$

From the relationship between $\omega_c(G)$ and $\tau(G)$ as stated in the previous section, it can be easily seen that

$$\sum_{s,t} M(s,t) a_s, b_t \leq 1$$

for all numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$ in [-1, 1].
From preposition 1, we have

$$\omega_q(G) - \tau(G) = [\omega_c - \tau(G)] \max_{|u_s\rangle |v_t\rangle} M(s,t) \langle u_s | v_t \rangle \leq K_G [\omega_c(G) - \tau(G)]$$

which is the required result.

The second case is when classical strategy performs well, but not perfectly. In this case, it is possible that the quantum strategy is quadratically better than classical one in terms of failure probability (as in case of odd cycle game).

The paper states that for an XOR game G with classical value $\omega_c(G)$, $\omega_q(G) \leq g(\omega_c(G))$, where g is a concave function defined as

$$g(\omega_c(G)) = \begin{cases} \gamma_1 \omega_c(G) & \text{if } \omega_c(G) \leq \gamma_2 \\ \sin^2(\frac{\pi}{2} \omega_c(G)) & \text{if } \omega_c(G) > \gamma_2 \end{cases} \tag{5}$$

where $\gamma_1 \approx 1.1382$ and $\gamma_2 \approx 0.74202$

The function g is chosen such that it is minimal subject to being concave and bounded below by $\sin^2 \frac{\pi}{2}x$. $\gamma_1 x$ is the tangent to $\sin^2 \frac{\pi}{2}x$ at the point $x = \gamma_2$. Thus the above chosen g is minimal, concave and bounded below by $\sin^2 \frac{\pi}{2}x$ (as above γ_2, $\sin^2 \frac{\pi}{2}x$ itself is concave and below it, g is a straight line which is minimally concave).

The above result has been proved by taking any optimal quantum strategy and defining a classical strategy based on that, in which instead of the entangled state, Alice and Bob share a randomly chosen unit vector. So let

$$|u_s\rangle : s \in S, |v_t\rangle : t \in T \subset \mathbb{R}^m$$

be the unit vectors associated with some optimal quantum strategy (acc. to proposition 5). Now a classical strategy is defined using these vectors:

1. Alice and Bob share a unit vector $\lambda \in \mathbb{R}^m$, chosen uniformly at random
2. When asked question s, Alice answers $a' = [1 + sign(\langle\lambda|u_s\rangle)]/2$
3. When asked question t, Bob answers $b' = [1 + sign(\langle\lambda|v_t\rangle)]/2$

To get the probability of winning, we need the probability with which $a' \oplus b' = 1$. This was done by introducing an azimuthal coordinate ϕ for $|\lambda\rangle$ in the plane spanned by $|u_s\rangle$ and $|v_t\rangle$ such that the coordinate for $|u_s\rangle$ is 0 and for v_s is $\theta_{st} = \cos^{-1}\langle u_s|v_t\rangle \in [0, \pi]$. Then $sign(\langle\lambda|u_s\rangle)$ is 1 for $\phi \in [-\pi/2, \pi/2]$ and -1 otherwise. Similarly, $sign(\langle\lambda|v_t\rangle)$ is 1 for $\phi \in [\theta_{st} - \pi/2, \theta_{st} + \pi/2]$ and -1 otherwise. Since $|\lambda\rangle$ is distributed uniformly in $\mathbb{R}^m$, ϕ is also distributed uniformly in $[0, 2\pi)$. Thus the probability with which $sign(\langle\lambda|u_s\rangle) = -sign(\langle\lambda|v_t\rangle)$ is the probability that $\phi \in [pi/2, \theta_{st} - \pi/2) \cup (\pi/2, \theta_{st} + \pi/2]$ which is $\frac{1}{\pi}\theta_{st}$.

Thus on input (s, t),

$$Pr[a' \oplus b' = 1] = \frac{1}{\pi}\theta_{st}$$

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

$$Pr[a \oplus b = 1] = \frac{1}{2}(1 - \langle u_s|v_t\rangle) \text{ (shown in proposition 1) } = \sin^2 \frac{1}{2}\theta_{st}$$

Thus,

$$Pr[a \oplus b = 1] = \sin^2(\frac{\pi}{2}Pr[a' \oplus b' = 1]) \leq g(Pr[a' \oplus b' = 1])$$

from properties of g. Similar result can be found for $a \oplus b = 0$.

For each $(s, t) \in S \times T$, let $\omega_c(s, t)$ and $\omega_q(s, t)$ be the probabilities of winning the game when using the above strategies given the question (s, t) was asked. The probability with winning with the quantum strategy is

$$\sum_{s,t} \pi(s,t)\omega_q(s,t) \leq \sum_{s,t} \pi(s,t)g(\omega_c(s,t)) \text{ (from above results) } \leq g\left(\sum_{s,t} \pi(s,t)\omega_c(s,t)\right) \text{ (from concavity of g) } \leq g(\omega_c(G))$$

3.5 Bounds on entanglement for XOR games

For any XOR game, G with $m = \min(|S|, |T|)$, there exists an optimal strategy for Alice and Bob in which they share a maximally-entangled state on $\lceil m/2 \rceil$ qubits.

The number of qubits is exponential in the size of their inputs But a sub-optimal strategy can be obtained using a polynomial number of shared qubits. This follows from the Johnson-Lindenstrauss lemma [6] :
For $\epsilon \in (0, 1)$ and n a positive integer, let K be a positive integer such that

$$K \geq 4(\epsilon^2/2 - \epsilon^3/3)^{-1} \log n \tag{6}$$

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

$$(1 - \epsilon)|||u\rangle - |v\rangle||^2 \leq ||f(|u\rangle) - f(|v\rangle)||^2 \leq (1 + \epsilon)|||u\rangle - |v\rangle||^2 \tag{7}$$

Using the lemma, we can arrive at the theorem,
Let $G = G(V, \pi)$ be an XOR game with quantum value $\omega_q(G)$. Let $0 < \epsilon < 1/10$, and suppose K is an even integer such that

$$K \geq 4(\epsilon^2/2 - \epsilon^3/3)^{-1} \log(|S| + |T| + 1) \tag{8}$$

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

Oded Regev has described to us an improved form of this theorem where K has no dependence on $|S|$ and $|T|$.

4 Conclusion

We need to study the upper bounds on quantum values of games as they are related to the soundness property of multi-prover interactive proof systems. For example, in the case of the Odd Cycle Game (a simple proof system for the two-colorability of odd cycles), the correct response for the verifier is to reject. This is valid for a classical system, but if the quantum value of the game were to be 1, then it would not be a valid *quantum-proof system*. The upper bound on the quantum value proves that it is a valid quantum proof system, and with a polynomial number of repetitions, the probability of the verifier incorrectly accepting the game can be made 0. Similarly, applying upper bounds on the number of entangled qubits helps in analyzing the complexity class of such systems.

For $0 \leq s < c \leq 1$, we define $\oplus\text{MIP}_{c,s}[10]$ denote the class of all languages L recognized by classical one-round two-prover interactive proof systems such that the verifier's decision is a function of parity of two bits sent by the provers (one each). If $x \notin L$, then the prover's acceptance probability is atmost the soundness probability, denoted by s, independent of the strategy followed by Alice and Bob. And if $x \in L$, there exists a strategy for which the prover's acceptance probability is atleast the completeness probability, denoted by c. Similarly, $\oplus\text{MIP}^*_{c,s}[10]$ denote same class of languages, with the difference that provers may share a prior entangled state. Then we get the following results -

- For all $\epsilon \in (0, 1/16)$, if $s = 11/16 + \epsilon$ and $c = 12/16$ then $\oplus\text{MIP}_{c,s}[10] = \text{NEXP}$
- For all s and c such that $0 \leq s < c \leq 1$, $\text{MIP}_{c,s}[10] \subseteq \text{EXP}$

References

[1] Alexander Grothendieck. "Résumé des résultats essentiels dans la théorie des produits tensoriels topologiques et des espaces nucléaires". fr. In: *Annales de l'Institut Fourier* 4 (1952), pp. 73–112. DOI: 10.5802/aif.46. URL: http://www.numdam.org/articles/10.5802/aif.46/.

[2] J. S. Bell. "On the Einstein Podolsky Rosen paradox". In: *Physics Physique Fizika* 1 (3 Nov. 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195. URL: https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195.

[3] John F. Clauser et al. "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Phys. Rev. Lett.* 23 (15 Oct. 1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880. URL: https://link.aps.org/doi/10.1103/PhysRevLett.23.880.

[4] J. L. Krivine. "Constantes de Grothendieck et fonctions de type positif sur les sphères". In: (1979).

[5] A.M. Davie. "Lower bound for K_G". In: (1984).

[6] William B. Johnson. "Extensions of Lipschitz mappings into Hilbert space". In: *Contemporary mathematics* 26 (1984), pp. 189–206.

[7] "Tsirel'son, B.S. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. J Math Sci 36, 557–570 (1987). https://doi.org/10.1007/BF01663472". In: (1987).

[8] N. David Mermin. "Simple unified form for the major no-hidden-variables theorems". In: *Phys. Rev. Lett.* 65 (27 Dec. 1990), pp. 3373–3376. DOI: 10.1103/PhysRevLett.65.3373. URL: https://link.aps.org/doi/10.1103/PhysRevLett.65.3373.

[9] N. David Mermin. "Hidden variables and the two theorems of John Bell". In: *Reviews of Modern Physics* 65.3 (July 1993), pp. 803–815. DOI: 10.1103/revmodphys.65.803. URL: https://doi.org/10.1103%2Frevmodphys.65.803.

[10] Andris Ambainis. "A New Protocol and Lower Bounds for Quantum Coin Flipping". In: *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*. STOC '01. Hersonissos, Greece: Association for Computing Machinery, 2001, pp. 134–142. ISBN: 1581133499. DOI: 10.1145/380752.380788. URL: https://doi.org/10.1145/380752.380788.

[11] "P. K. Aravind. The magic squares and Bell's theorem. Manuscript, 2002. Available as arXiv.org e-Print quant-ph/0206070." In: (2002).