Advantage of Quantum Strategies in Random Symmetric XOR Games

Andris Ambainis*, Jānis Iraids**, Dmitry Kravchenko***, and Madars Virza†

Faculty of Computing, University of Latvia

Abstract. Non-local games are known as a simple but useful model which is widely used for displaying nonlocal properties of quantum mechanics. In this paper we concentrate on a simple subset of non-local games: multiplayer XOR games with 1-bit inputs and 1-bit outputs which are symmetric w.r.t. permutations of players.

We look at random instances of non-local games from this class. We prove a tight bound for the expected performance on the classical strategies for a random non-local game and provide numerical evidence that quantum strategies achieve better results.

1 Introduction

Non-local games [CHTW04] are studied in quantum information, with the goal of understanding the differences between quantum mechanics and classical physics. An example of non-local game is the CHSH (Clauser-Horne-Shimoni-Holt) game [CHSH69, CHTW04]. This is a game played by two parties against a referee. The referee prepares two uniformly random bits x, y and gives one of them to each of two parties. The two parties cannot communicate but can share common randomness or a common quantum state that is prepared before the beginning of the game. The parties reply by sending bits a and b to the referee. They win if $a \oplus b = x \wedge y$.

The maximum winning probability that can be achieved in the CHSH game is 0.75 classically and $\frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.85...$ quantumly. This is interesting because it provides a simple experiment for testing the validity of quantum mechanics. Assume that we implement the referee and the players by devices so that the communication between the players is clearly excluded. If the experiment is repeated m times and players win substantially more than $0.75m$ times, then the results of experiment can be explained using quantum mechanics but not through classical physics.

More generally, we can study non-local games with N players. The referee prepares inputs $x_1, \ldots, x_N$ by picking $(x_1, \ldots, x_N)$ according to some probability

* Supported by ESF project 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044.

** Supported by FP7 FET-Open project QCS.

*** Supported by ESF graduate fellowship.

† Since September 2011, at the Department of EECS, Massachussets Institute for Technology. Supported by FP7 FET-Open project QCS during this research.

A. Kučera et al. (Eds.): MEMICS 2012, LNCS 7721, pp. 57–68, 2013.

distribution and sends x_i to the i^{th} player. The i^{th} player replies to sending an answer y_i to the referee. Players win if their answers $y_1, \ldots, y_N$ satisfy some winning condition $P(x_1, \ldots, x_N, y_1, \ldots, y_N)$. Similarly as before, the players cannot communicate but can use shared random bits or a common quantum state that has been prepared before receiving $x_1, \ldots, x_N$ from the referee.

Non-local games have been a very popular research topic (often, under the name of Bell inequalities [Be64]). Many non-local games have been studied and large gaps between classical and quantum winning probabilities have been discovered (e.g., [Me90, BV11, BRSW11]).

In this paper, we study non-local games for which the winning condition $P(x_1, \ldots, x_N, y_1, \ldots, y_N)$ is chosen randomly from some class of possible winning conditions. This direction of study was started by [ABB+12] which studied random XOR games with 2 players (players receive inputs $x_1, x_2 \in \{1, \ldots, m\}$ and provide outputs $y_1, y_2 \in \{0, 1\}$, the winning condition depends on x_1, x_2 and $y_1 \oplus y_2$) and showed that, for a random game in this class, its quantum value[1] is between 1.2011... and 1.5638... times its classical value.

We look at a different class of games: N player symmetric XOR games with binary inputs [AKNR09]. For games in this class, both inputs $x_1, \ldots, x_N$ and outputs $y_1, \ldots, y_N$ are binary. The winning condition may depend on the number of $i : x_i = 1$ and the parity of all outputs $\oplus_{i=1}^{N} y_i$. This class of non-local games contains some games with a big quantum advantage. For example, Mermin-Ardehali inequality [Me90, Ar92] can be recast into an N-partite symmetric XOR game whose quantum value is $2^{\lceil \frac{N}{2} - 1 \rceil - \frac{1}{2}}$ times bigger than its classical value.

We show that quantum strategies have some advantage even for a random non-local game from this class:

- We present results of computer experiments that clearly indicate an advantage for quantum strategies.
- We prove that the expected classical value of a random N-player symmetric XOR game is $\frac{0.8475...}{\sqrt[4]{N}}$.
- We provide a non-rigorous argument that the quantum value is $\Omega(\frac{\sqrt{\log N}}{\sqrt[4]{N}})$, with a high probability.

This quantum advantage is, however, much smaller than the maximum advantage achieved by the Mermin-Ardehali game.

2 Definitions

We consider non-local games of N players. We assume that players are informed about the rules of the game and are allowed to have a preliminary discussion. When the game is started, players receive a uniformly random input $x_1, \ldots, x_N \in$

[1] Quantum (classical) value of a game is the maximum difference between the winning probability and the losing probability that can be achieved by quantum (classical) strategies.

$\{0,1\}$ with the i^{th} player receiving x_i. The i^{th} player then produces an output $y_i \in \{0,1\}$. No communication is allowed between the players but they can use shared randomness (in the classical case) or quantum entanglement (in the quantum case).

In an XOR game, the winning condition $P(x_1,\ldots,x_N,y_1,\ldots,y_N)$ depends only on $x_1,\ldots,x_N$ and the overall parity of all the output bits $\oplus_{i=1}^{N} y_i$. A game is symmetric if the winning condition does not change if $x_1,\ldots,x_N$ are permuted.

If an XOR game is symmetric, the winning condition depends only on $\sum_{i=1}^{N} x_i$ and $\oplus_{i=1}^{N} y_i$. Thus, we can define the rules of a game as a sequence of $N+1$ bits $G = G_0 G_1 \ldots G_N$, where G_j defines a "winning" value of $\oplus_{i=1}^{N} y_i$ for input with $\sum_{i=1}^{N} x_i = j$.

By a random N-player symmetric XOR game we shall mean a game defined by the $(N+1)$-bit string $G = G_0 G_1 \ldots G_N$ picked uniformly at random.

Let $\Pr_{win}(S)$ and $\Pr_{loss}(S)$ be the probabilities that players win (lose) the game when playing according to a strategy S (which can be either a classical or a quantum strategy). The *value of a strategy* S for a game is $Val(S) = \Pr_{win}(S) - \Pr_{loss}(S)$.The *value of a game* $Val(G) = \max_S Val(S)$ is the value of an optimal (or a best) strategy for this game.

We use Val_C to denote the classical value (maximum of the value over classical strategies) and Val_Q to denote the quantum value (maximum of the value over classical strategies). We omit the subscript C or Q if it is clear from the context whether we are considering quantum or classical value.

3 Optimal Strategies

3.1 Classical Games

Without a loss of generality, we can assume that in a classical game all players use deterministic strategies. (If a randomized strategy is used, we can fix the random bits to the values that achieve the biggest winning probability. Then, a randomized strategy becomes deterministic.)

Then, each player has four different choices — (00), (01), (10), (11). (The first bit here represents the answer on input 0, and second bit represents the answer on input 1. Thus, (ab) denotes a choice to answer a on input 0 and answer b on input 1.)

We use $(00)^{k_0}\,(01)^{k_1}\,(10)^{k_2}\,(11)^{k_3}$ to denote a strategy for N players in which k_0 players use (00), k_1 players use (01), k_2 players use (10) and k_3 players use (11).

Let S be an arbitrary strategy for N players. If exactly one of the players inverts his choice of a strategy bitwise (e.g. $(11) \rightarrow (00)$, or $(10) \rightarrow (01)$), this leads to the parity of output bits $\oplus_{i=1}^{N} y_i$ always being opposite compared to the original strategy. Hence, if $\overline{S}$ is the new strategy, then $\overline{S}$ wins whenever S loses and $\overline{S}$ loses whenever S wins. Therefore,

$$Val(S) = \Pr_{win}(S) - \Pr_{loss}(S) = \Pr_{loss}(\overline{S}) - \Pr_{win}(\overline{S}) = -Val\left(\overline{S}\right).$$

From now on, we consider such strategies S and $\overline{S}$ (with exactly one player's choice bitwise inverted) together with a positive value $|Val\,(S)| = \left|Val\,(\overline{S})\right|$.

Theorem 1. *[AKNR09] Let S be any classical strategy for a symmetric XOR game with binary inputs. Then, $Val(S)$ is the same as the value of one of $N+1$ following strategies:*

$$(00)^k\,(01)^{N-k}\,, \text{where } k \in \{0, 1, \ldots, N\}. \tag{1}$$

This allows to restrict the set of strategies considerably. In fact, the most useful strategies are $(00)^N$ and $(01)^N$. In our computer experiments, one of these strategies is optimal for $\approx$ 99% symmetric XOR games. Our rigorous results in Section 5 imply that asymptotically (in the limit of large N) the fraction of games for which one of these strategies is optimal is $1 - o(1)$.

3.2 Quantum Games

The setting in quantum game is identical to the classical one except that the players are allowed to use a quantum system which is potentally entangled before the start of the game. There are two notable results that significantly help the further analysis.

Firstly, it was shown by Werner and Wolf in [WW01] and [WW01a] that in the more general setting where games are not necessarily symmetric the value of the game is described by a simple expression. Let the game be specified by

$$c_{x_1,x_2,\ldots,x_N} = \begin{cases} 1, & \text{if players win when } y_1 \oplus \ldots \oplus y_N = 1 \\ -1, & \text{if players win when } y_1 \oplus \ldots \oplus y_N = 0 \end{cases}$$

Theorem 2

$$Val_Q(G) = \max_{\substack{\lambda_1,\ldots,\lambda_N \in \mathbb{C}, \\ |\lambda_1| = \ldots = |\lambda_N| = 1}} \left| \sum_{x_1,\ldots,x_N \in \{0,1\}} \frac{c_{x_1,\ldots,x_N} \lambda_1^{x_1} \cdots \lambda_N^{x_N}}{2^N} \right|$$

Secondly, for symmetric games the expression was simplified further in [AKNR09]. Denoting again for convenience $c_j = (-1)^{G_j}$:

Theorem 3

$$Val_Q(G) = \max_{\substack{\lambda \in \mathbb{C}, \\ |\lambda| = 1}} \left| \sum_{j=0}^{N} \frac{c_j \binom{N}{j} \lambda^j}{2^N} \right|$$

4 Computer Experiments

On the ground of Theorems 1 and 3 we have built efficient optimization algorithms in order to show the difference between classical and quantum versions of symmetric XOR games.

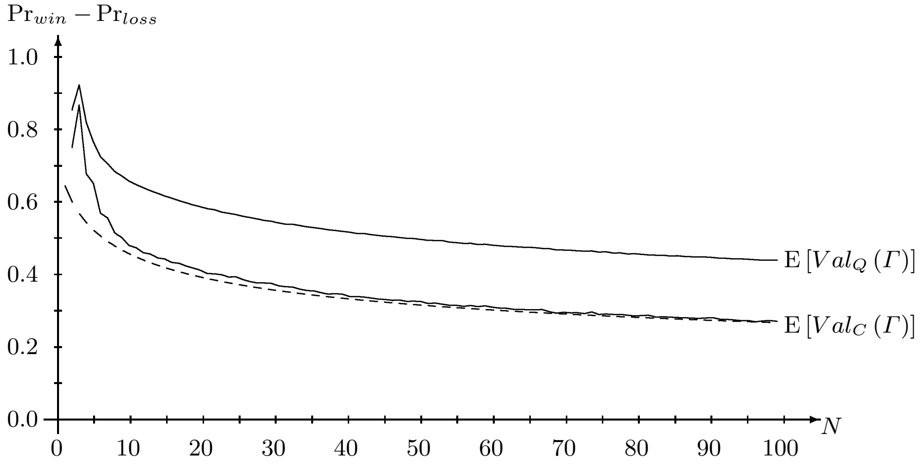

Fig. 1. Expected values of quantum and classical XOR games + classical bound

The Figure 1 shows the expected classical and quantum values for a randomly chosen symmetric XOR game with binary inputs, with the number of players N ranging between 2 and 101[2]. Dashed graph corresponds to the function $f(N) = \frac{0.8475...}{\sqrt[4]{N}}$ derived from Theorem 4.

We see that there is a consistent quantum advantage for all N.

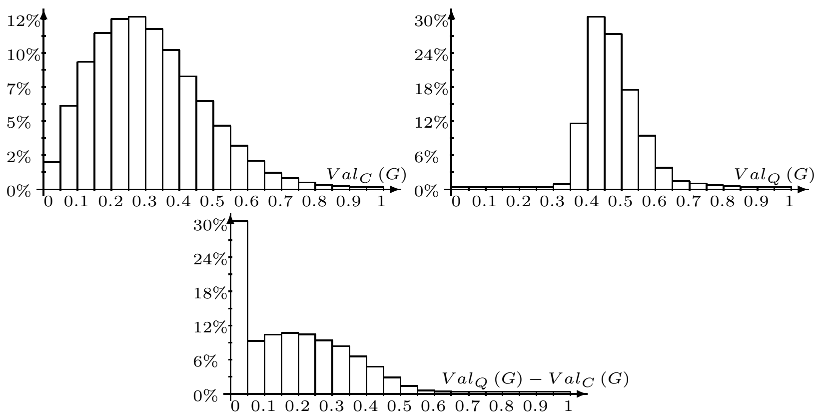

Fig. 2. Histograms of values of random 64-player symmetric XOR games

In the Figure 2, we provide some statistical data on the distribution of the game values (from 10^6 randomly selected games for $N = 64$). The first two

[2] For $N \leq 16$ graphs are precise, as for small number of players it was possible to analyze all 2^{N+1} games. For $N > 16$ we picked 10^5 games at random for each N.

histograms show the distribution of classical and quantum values, respectively. The last one shows the distribution of biases between the values of classical and quantum versions of a game.

We see that the quantum value of a game is more sharply concentrated than the classical value. There is a substantial number (around 30%) of games which have no quantum advantage (or almost no quantum advantage)[3]. For the remaining games, the gap between quantum and classical values is quite uniformly distributed over a large interval.

5 Bounding Classical Game Value

5.1 Results

In this section we first obtain a tight bound on the value of strategies $(00)^N$ and $(01)^N$.

Theorem 4. *For a random N-player symmetric XOR game with binary inputs,*

$$\mathrm{E}\left[\max\left(\left|Val\left((00)^N\right)\right|, \left|Val\left((01)^N\right)\right|\right)\right] = \frac{0.8475... + o(1)}{\sqrt[4]{N}}.$$

We then show that any other strategy from (1) gives a weaker result, with a high probability.

Theorem 5. *For any $c > 0$,*

$$\Pr\left[\max_{k:1\leq k\leq N-1}\left|Val\left((00)^k\,(01)^{N-k}\right)\right| \geq \frac{c}{\sqrt[4]{N}}\right] = O\left(\frac{1}{N}\right).$$

5.2 Proof of Theorem 4

We first consider the strategy $(00)^N$. As all players always answer 0, the value of this strategy is equal to

$$Val\left((00)^N\right) = \sum_{j=0}^{N}\frac{(-1)^{G_j}\binom{N}{j}}{2^N} \tag{2}$$

For the strategy $(01)^N$, we have

$$Val\left((01)^N\right) = \left|\sum_{j=0}^{N}\frac{(-1)^{G_j+j}\binom{N}{j}}{2^N}\right| \tag{3}$$

We need to find a bound for

$$\mathrm{E}\left[\max\left(\left|Val\left((00)^N\right)\right|, \left|Val\left((01)^N\right)\right|\right)\right]$$

[3] However, our results in the next sections indicate that the fraction of such games will tend to 0 for larger N.

$$= \mathrm{E}\left[\max\left(\left|\sum_{j=0}^{N}\frac{(-1)^{G_j}\binom{N}{j}}{2^N}\right|,\left|\sum_{j=0}^{N}\frac{(-1)^{G_j+j}\binom{N}{j}}{2^N}\right|\right)\right] \tag{4}$$

Among the summands of these two sums let us first evaluate those which are equal for both of sums, i.e. for even j's, and then for remaining summands, which have opposite values in these sums, i.e. for odd j's:

$$\mathrm{E}\left[\max\left(\left|Val\left((00)^N\right)\right|,\left|Val\left((01)^N\right)\right|\right)\right]$$

$$= \mathrm{E}\left[\max\left(\pm\sum_{\substack{0\le j\le N,\\ j \text{ is even}}}\frac{(-1)^{G_j}\binom{N}{j}}{2^N}\pm\sum_{\substack{0\le j\le N,\\ j \text{ is odd}}}\frac{(-1)^{G_j}\binom{N}{j}}{2^N}\right)\right]$$

$$= \mathrm{E}\left[\left|\sum_{\substack{0\le j\le N,\\ j \text{ is even}}}\frac{(-1)^{G_j}\binom{N}{j}}{2^N}\right|\right]+\mathrm{E}\left[\left|\sum_{\substack{0\le j\le N,\\ j \text{ is odd}}}\frac{(-1)^{G_j}\binom{N}{j}}{2^N}\right|\right] \tag{5}$$

Let Σ_{even} and Σ_{odd} be the two sums in (5). Then, we have

$$\mathrm{Var}\left[\Sigma_{even}\right] = \sum_{\substack{0\le j\le N,\\ j \text{ is even}}}\left(\frac{\binom{N}{j}}{2^N}\right)^2 = \frac{\binom{2N}{N}}{2\cdot 4^N}.$$

Similarly, $\mathrm{Var}\left[\Sigma_{odd}\right] = \frac{\binom{2N}{N}}{2\cdot 4^N}$. From the central limit theorem, in the limit of large N, each of random variables Σ_{even} and Σ_{odd} can be approximated by a normally distributed random variable with the same mean (which is 0) and variance. If X is a normally distributed random variable with $E[X] = 0$, then $E[|X|] = \sqrt{\frac{2}{\pi}}\sqrt{\mathrm{Var}[X]}$. Hence, (5) is equal to

$$\mathrm{E}\left[|\Sigma_{even}|\right] + \mathrm{E}\left[|\Sigma_{odd}|\right]$$

$$= \sqrt{\frac{2}{\pi}}(1+o(1))\sqrt{\mathrm{Var}\left[\Sigma_{even}\right]} + \sqrt{\frac{2}{\pi}}(1+o(1))\sqrt{\mathrm{Var}\left[\Sigma_{odd}\right]}$$

$$= (1+o(1))\sqrt{\frac{2}{\pi}}\sqrt{\frac{2\binom{2N}{N}}{4^N}} = (1+o(1))\sqrt[4]{\frac{16}{\pi^3}}\frac{1}{\sqrt[4]{N}} = \frac{0.8475...+o(1)}{\sqrt[4]{N}}$$

where the second-to-last equality follows from the approximation of the binomial coefficients $\binom{2N}{N} = (1+o(1))\frac{4^N}{\sqrt{\pi N}}$.

5.3 Variance of Other Strategies

We now consider other strategies S, with the goal of proving Theorem 5. To do that, we first compute the variances for their values $Val(S)$. (Our goal is to prove Theorem 5 by Chebyshev's inequality, which we do in the next subsection.)

We start with the variance of $Val((00)^N)$. Because of (2), the variance of $Val((00)^N)$ can be calculated as

$$\mathrm{Var}\left[Val\left((00)^N\right)\right] = \sum_{j=0}^{N} \mathrm{Var}\left[\frac{(-1)^{G_j}\binom{N}{j}}{2^N}\right] = \sum_{j=0}^{N} \frac{\binom{N}{j}^2}{4^N} = \frac{\binom{2N}{N}}{4^N} \approx \frac{1}{\sqrt{\pi N}} \quad (6)$$

We note that $Val\left((00)^N\right)$ for the game $G_0G_1G_2G_3G_4\ldots$ is exactly the same as $Val\left((01)^N\right)$ for the game $G_0\overline{G_1}G_2\overline{G_3}G_4\ldots$, with all odd bits inverted.

More generally, assume that we have a strategy $(00)^k\,(01)^{N-k}$. We can invert the answers by all players for the case $x_i = 1$. Then, the overall parity of answers $\oplus_{i=1}^N y_i$ stays the same if an even number of players have received $x_i = 1$ and changes to opposite value if an odd number of players have received $x_i = 1$. If we simultaneously invert all odd-numbered bits G_i in the winning condition, the game value does not change. From this, we conclude that for each k,

$$Val\left((00)^k\,(01)^{N-k}\right) = Val\left((00)^{N-k}\,(01)^k\right) \quad (7)$$

We now consider the value for the second strategy from (1), $(00)^{N-1}\,(01)$, for a random symmetric XOR game.

Probability distribution of $\oplus_{i=0}^N y_i$ when $\sum_{i=0}^N x_i = j$ is the following:

j	0	1	2	3	4	5	6	7	...
$\Pr\left[\oplus_{i=0}^N y_i = 0\right]$	1	$\frac{1}{N}$	$\frac{N-2}{N}$	$\frac{3}{N}$	$\frac{N-4}{N}$	$\frac{5}{N}$	$\frac{N-6}{N}$	$\frac{7}{N}$	...
$\Pr\left[\oplus_{i=0}^N y_i = 1\right]$	0	$\frac{N-1}{N}$	$\frac{2}{N}$	$\frac{N-3}{N}$	$\frac{4}{N}$	$\frac{N-5}{N}$	$\frac{6}{N}$	$\frac{N-7}{N}$	...

Given input with $\sum_{i=0}^N x_i = j$, the strategy outputs even or odd answer, depending on whether or not the last player has received 1, i.e. with probabilities $\frac{N-j}{N}$ and $\frac{j}{N}$ (unlike 1 and 0 in the case of symmetric strategies).

Therefore, variance of the strategy $(00)^{N-1}\,(01)$ for input with $\sum_{i=0}^N x_i = j$ is $\left(\frac{N-j}{N} - \frac{j}{N}\right)^2 = \left(\frac{N-2j}{N}\right)^2$.

Summing up variances for all possible j's, we get

$$\begin{aligned}\mathrm{Var}\left[Val\left((00)^{N-1}\,(01)\right)\right] &= \sum_{j=0}^{N} \mathrm{Var}\left[\frac{\pm\frac{N-2j}{N}\binom{N}{j}}{2^N}\right] \\ &= \sum_{j=0}^{N}\left(\frac{\pm\frac{N-2j}{N}\binom{N}{j}}{2^N}\right)^2 = \frac{\binom{2N}{N}}{4^N\,(2N-1)} \approx \frac{1}{\sqrt{\pi N}\,(2N-1)},\end{aligned} \quad (8)$$

with the third equality following from Lemma 1 in the appendix (Notation $\pm\frac{N-2j}{N}$ denotes a random variable with equiprobable values $+\frac{N-2j}{N}$ and $-\frac{N-2j}{N}$.)

Due to (7), the value of strategy $(00)(01)^{N-1}$ has the same variance.

Other strategies of type $(00)^{N-k}(01)^k$ where $2 \le k \le N-2$ have much smaller variances, which can be expressed as follows:

$$\begin{aligned}\mathrm{Var}\left[Val\left((00)^{N-k}(01)^k\right)\right] &= \sum_{j=0}^{N}\left(\frac{\left(\sum_{l=0}^{j}(-1)^l\frac{\binom{k}{l}\binom{N-k}{j-l}}{\binom{N}{j}}\right)\binom{N}{j}}{2^N}\right)^2 \\ &= \frac{\sum_{j=0}^{N}\left(\sum_{l=0}^{j}(-1)^l\binom{k}{l}\binom{N-k}{j-l}\right)^2}{4^N}\end{aligned} \tag{9}$$

The expression $\sum_{l=0}^{j}(-1)^l\binom{k}{l}\binom{N-k}{j-l}$ inside (9) is well known Kravchuk polynomial $K_j(k)$, whose square can be bounded by strict inequality provided in [Kr01]:

$$\left(\sum_{l=0}^{j}(-1)^l\binom{k}{l}\binom{N-k}{j-l}\right)^2 = (K_j(k))^2 < 2^N\binom{N}{j}\binom{N}{k}^{-1}. \tag{10}$$

This inequality implies that

$$\begin{aligned}\mathrm{Var}\left[Val\left((00)^{N-k}(01)^k\right)\right] &= \frac{\sum_{j=0}^{N}(K_j(k))^2}{4^N} \\ &< \frac{\sum_{j=0}^{N}2^N\binom{N}{j}\binom{N}{k}^{-1}}{4^N} = \binom{N}{k}^{-1}.\end{aligned} \tag{11}$$

5.4 Proof of Theorem 5

Among the strategies $(00)^k(01)^{N-k}$, $k \in \{1, \ldots, N-1\}$, two strategies (for $k = 1$ and $k = N-1$) have variance $\approx \frac{1}{\sqrt{\pi N}(2N-1)}$, and the remaining $N-3$ strategies have variance less than $\frac{1}{\binom{N}{k}}$.

We now apply Chebyshev inequality, using those two bounds on the variance. We have

$$\begin{aligned}&\Pr\left[\left|Val\left((00)^{N-1}(01)\right)\right| \ge \frac{\lambda}{\sqrt[4]{\pi N}\sqrt{2N-1}}\right] \\ &\qquad = \Pr\left[\left|Val\left((00)(01)^{N-1}\right)\right| \ge \frac{\lambda}{\sqrt[4]{\pi N}\sqrt{2N-1}}\right] \le \frac{1}{\lambda^2},\end{aligned}$$

and, for $2 \le k \le N-2$:

$$\Pr\left[\left|Val\left((00)^{N-k}(01)^k\right)\right| \ge \frac{\lambda}{\sqrt{\binom{N}{k}}}\right] \le \frac{1}{\lambda^2}. \tag{12}$$

We now combine the bounds (12) into one upper bound.

$$\Pr\left[\max_{0\le k\le N}\left|Val\left((00)^{N-k}(01)^k\right)\right|\ge B\right]\le$$
$$\le 2\times\frac{1}{\left(B\sqrt[4]{\pi N}\sqrt{(2N-1)}\right)^2}+\sum_{k=2}^{N-2}\frac{1}{\left(B\sqrt{\binom{N}{k}}\right)^2}$$
$$=\frac{2}{B^2\sqrt{\pi N}\,(2N-1)}+O\left(\frac{1}{B^2N^3}\right),\quad (13)$$

with the last equality following from $\binom{N}{k}\ge\binom{N}{2}$ and the fact that we are summing over $N-3$ values for k: $k\in\{2,\ldots,N-2\}$. Taking $B=\frac{c}{\sqrt[4]{N}}$ proves theorem 5.

6 Bounding Quantum Game Value

So far we have not been able to find a tight lower bound on the mean value of the game in quantum case. However, we provide some insights which could lead to a solution to the problem. We can bound the value from below by

$$\max_{\substack{\lambda\in\mathbb{C},\\|\lambda|=1}}\left|\sum_{j=0}^{N}\frac{c_j\binom{N}{j}\lambda^j}{2^N}\right|\ge\max_{\alpha}\left|\sum_{j=0}^{N}\frac{c_j\binom{N}{j}\cos(\alpha j)}{2^N}\right| \quad (14)$$

The sum $\sum_{j=0}^{N}c_j\cos(\alpha j)$ where c_j are indepedent random variables with mean 0 and variance 1 has been extensively studied under the name "random trigonometric polynomials" by Salem and Zygmund[SZ54] and others. Their results imply that there exist constants A and B such that

$$\lim_{M\to\infty}\Pr\left[A\sqrt{M\log M}\le\max_{\alpha}\left|\sum_{j=0}^{M}c_j\cos(\alpha j)\right|\le B\sqrt{M\log M}\right]=1 \quad (15)$$

To apply (15), the crucial step is to reduce a sum $c_j\binom{N}{j}\cos(\alpha j)$ with binomial coefficients to a sum $c_j\cos(\alpha j)$ not containing binomial coefficients.

We propose a following non-rigorous approximation. We first drop the terms with $j\le\frac{N}{2}-\sqrt{N}$ and $j\ge\frac{N}{2}-\sqrt{N}$. For the remaining terms, we replace $\binom{N}{j}$ with $\binom{N}{N/2}$ (since $\binom{N}{j}=\Theta(\binom{N}{N/2})$ for $j\in[\frac{N}{2}-\sqrt{N},\frac{N}{2}+\sqrt{N}]$). If this approximation can be justified, it reduces (14) to (15) with $M=2\sqrt{N}$. This would lead to a lower bound of

$$E_G[Val_Q(G)]=\Omega\left(\frac{\sqrt{\log M}}{\sqrt{M}}\right)=\Omega\left(\frac{\sqrt{\log N}}{\sqrt[4]{N}}\right).$$

We are currently working on making this argument rigorous.

7 Conclusion

We studied random instances of symmetric N-player XOR games with binary inputs, obtaining tight bounds for the classical value of such games. We also presented a non-rigorous argument bounding the quantum value. Our results indicate that quantum strategies are better than classical for random games in this class, by a factor of $\Omega(\sqrt{\log N})$. An immediate open problem is to make our bound for quantum strategies precise, by bounding the error introduced by our approximations.

A more general question is: can we analyze random instances of other classes of non-local games? We currently know how to analyze random games for 2-player XOR games with N-valued inputs and for symmetric N-player games with binary inputs.

Can we analyze, for example, 3-player XOR games with N-valued inputs? In a recent work, Briët and Vidick [BV11] have shown big gaps between quantum and classical strategies for this class of games. However, methods of analyzing such games are much less developed and this makes analysis of random games quite challenging. Developing tools for it is an interesting direction for future work.

References

[ABB+12] Ambainis, A., Bačkurs, A., Balodis, K., Kravčenko, D., Ozols, R., Smotrovs, J., Virza, M.: Quantum Strategies Are Better Than Classical in Almost Any XOR Game. In: Czumaj, A., Mehlhorn, K., Pitts, A., Wattenhofer, R. (eds.) ICALP 2012. LNCS, vol. 7391, pp. 25–37. Springer, Heidelberg (2012)

[AKNR09] Ambainis, A., Kravchenko, D., Nahimovs, N., Rivosh, A.: Nonlocal Quantum XOR Games for Large Number of Players. In: Kratochvíl, J., Li, A., Fiala, J., Kolman, P. (eds.) TAMC 2010. LNCS, vol. 6108, pp. 72–83. Springer, Heidelberg (2010)

[Ar92] Ardehali, M.: Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. Physical Review A 46, 5375–5378 (1992)

[Be64] Bell, J.: On the Einstein-Podolsky-Rosen paradox. Physics 1(3), 195–200 (1964)

[BV11] Briët, J., Vidick, T.: Explicit lower and upper bounds on the entangled value of multiplayer XOR games. arXiv:1108.5647

[BRSW11] Buhrman, H., Regev, O., Scarpa, G., de Wolf, R.: Near-Optimal and Explicit Bell Inequality Violations. In: Proceedings of CCC 2011, pp. 157–166 (2011)

[CHSH69] Clauser, J., Horne, M., Shimony, A., Holt, R.: Physical Review Letters 23, 880 (1969)

[CHTW04] Cleve, R., Høyer, P., Toner, B., Watrous, J.: Consequences and limits of nonlocal strategies. In: Proceedings of CCC 2004, pp. 236–249 (2004); Also quant-ph/0404076

[Kr01] Krasikov, I.: Nonnegative Quadratic Forms and Bounds on Orthogonal Polynomials. Journal of Approximation Theory 111, 31–49 (2001), doi:10.1006/jath.2001.3570

[Me90] Mermin, D.: Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States. Physical Review Letters 65(15) (1990)

[SZ54] Salem, R., Zygmund, A.: Some properties of trigonometric series whose terms have random signs. Acta Math. 91, 245–301 (1954)

[WW01] Werner, R.F., Wolf, M.M.: Bell inequalities and Entanglement. Quantum Information and Computation 1(3), 1–25 (2001)

[WW01a] Werner, R.F., Wolf, M.M.: All multipartite Bell correlation inequalities for two dichotomic observables per site. Physical Review A 64, 32112 (2001)

A Appendix

Lemma 1

$$\sum_{j=0}^{N}\left(\frac{N-2j}{N}\binom{N}{j}\right)^2 = \frac{\binom{2N}{N}}{2N-1}$$

Proof

$$\begin{aligned}
&\sum_{j=0}^{N}\left(\frac{N-2j}{N}\binom{N}{j}\right)^2 \\
&= \sum_{j=0}^{N}\left(1-4\frac{j}{N}+4\frac{j^2}{N^2}\right)\binom{N}{j}^2 \\
&= \sum_{j=0}^{N}\binom{N}{j}^2 - 4\sum_{j=1}^{N}\binom{N-1}{j-1}\binom{N}{j} + 4\sum_{j=1}^{N}\binom{N-1}{j-1}^2 \\
&= \binom{2N}{N} - 4\binom{2N-1}{N-1} + 4\binom{2N-2}{N-1} \\
&= \binom{2N}{N} - 2\binom{2N}{N} + \frac{2N}{2N-1}\binom{2N}{N} \\
&= \frac{\binom{2N}{N}}{2N-1}
\end{aligned}$$